



VCU

Virginia Commonwealth University
VCU Scholars Compass

Theses and Dissertations

Graduate School

2008

Shaping Strategic Information Systems Security Initiatives in Organizations

Gurvirender Tejay
Virginia Commonwealth University

Follow this and additional works at: <https://scholarscompass.vcu.edu/etd>



Part of the [Management Information Systems Commons](#)

© The Author

Downloaded from

<https://scholarscompass.vcu.edu/etd/1576>

This Dissertation is brought to you for free and open access by the Graduate School at VCU Scholars Compass. It has been accepted for inclusion in Theses and Dissertations by an authorized administrator of VCU Scholars Compass. For more information, please contact libcompass@vcu.edu.

© Gurvirender Pal Singh Tejay 2008

All Rights Reserved

**SHAPING STRATEGIC INFORMATION SYSTEMS
SECURITY INITIATIVES IN ORGANIZATIONS**

A dissertation submitted in fulfillment of the requirements for the degree of
Doctor of Philosophy in Business at Virginia Commonwealth University.

by

GURVIRENDER PAL SINGH TEJAY

Master of Science in Computer Science, University of Chicago, 2003

Master of Arts in Economics, University of Wisconsin – Milwaukee, 2002

Bachelor of Arts in Economics, University of Wisconsin – Milwaukee, 2000

Director: DR. GURPREET S DHILLON

PROFESSOR, DEPARTMENT OF INFORMATION SYSTEMS

Virginia Commonwealth University

Richmond, Virginia

August 2008

Acknowledgment

After grueling five years of pursuing my dissertation, which saw the high of early doctoral day's optimism and lows of hunting for free food even if it meant sitting in on Dean's research seminar on a beautiful Friday afternoon, I am tempted to wrap up this acknowledgment with one line - The life looks beautiful outside. However, the unforgiving lords of the doctoral program require one to pay homage to the life spent inside getting tanned by the glare of computer screen. So, the following is keeping with the sacred doctoral tradition.

I thank with all sincerity to my family for the faith and trust they reposed in me. My father and mother have been a source of inspiration and light in my life. I thank them for everything. I am grateful to my sister and wife for all the love, support and encouragement that helped me through the difficult stages of last few years. I am thankful to two bundles of joy - my nieces Ashriya and Ishrat. You have touched me in your own special way.

I recall with gratitude the guidance and support I have received from Dr. Gurpreet Dhillon, Dr. Allen Lee, and Dr. Richard Redmond. To my mentor and advisor, Dr Gurpreet Dhillon, I thank you for your patience and unwavering commitment to bring out the best in me. You have pushed me to work hard and achieve excellence by setting personal example. I have learned so much from you. I also sincerely acknowledge Dr. Allen Lee. I am grateful for your words of wisdom. I thank you for asking the hard questions and helping me crystallize my thoughts. You have a

wonderful ability to bring out the best in my work. Special thanks are in order for Dr. Richard Redmond. I thank you for having faith in my capabilities. You have supported me in different ways throughout the dissertation process. You have given me help and provided solution to every major problem I faced. I thank you for being there for me.

Thanks to my committee members for agreeing to take part in my dissertation journey. I thank Dr. Carolyn Strand Norman for discussing my dissertation, reading the chapters and providing useful comments. I appreciate your help and kindness. To Dr. Rajiv Kohli and Dr. Ramesh Shukla, I am grateful for your patience with my dissertation. You have stood with me and provided support when I needed it. I thank you with all sincerity.

Thanks are due to Dr. Edward Lieblein and Dr Sumitra Mukherjee. I thank you for having faith in my work and trusting me to complete the journey. I am grateful for your support without which the last part of my dissertation phase would have been very difficult. I also thank all my colleagues at the Nova Southeastern University.

To all my research participants, I thank you for your perspectives and time. Few individuals need special mention: Peggy Ward, Cathie Brown, Benny Ambler, Dr. Easton Rhodd, Robert Borter, Steve Kelliher and Jim Austin. This dissertation would not have been possible without your strong support.

I thank Stephen Pepper, Pierre Bourdieu and Anthony Giddens for leaving behind an intellectual legacy. This rich tradition is a source of inspiration and has helped me in my intellectual development.

To all my friends - the few and special, I thank you for tolerating me these last five years and listening to me. I promise to match your generosity and warmth with kind. I hope you all are proud of me.

This dissertation is dedicated to all those who thought I would not make it.

“Deh shiva var mohe hai shubh karman te kabhun na daroon,
na daroon ersoh jab chahe laroon, nishche kar apni jeet karoon.”
Guru Gobind Singh (1666 – 1708)

(Translation: With the blessings of the Almighty, I am not afraid to do good deeds and fight for them and I will ensure that I achieve victory)

Table of Contents

	Page
List of Tables	xii
List of Figures	xiii
Abstract.....	xiv
Chapter	
1 INTRODUCTION.....	1
1.1 Introduction	1
1.2 Nature of the research	2
1.3 Scope of the research	4
1.4 Structure of the dissertation	5
2 A CRITICAL REVIEW OF RESEARCH IN INFORMATION	
SYSTEMS SECURITY	7
2.1 Introduction	7
2.2 The intellectual map.....	8
2.3 Research in information systems security.....	12
Formism as world hypothesis	12
Mechanism as world hypothesis	19
Organicism as world hypothesis.....	28
Contextualism as world hypothesis.....	33
2.4 Discussion.....	37
2.5 Conclusion.....	42

3	RESEARCH METHODOLOGY	44
3.1	Introduction	44
3.2	Philosophical considerations	44
3.3	Theoretical considerations.....	47
	Research argument and questions.....	48
	Theoretical perspective	49
	Theoretical framework to conduct argument.....	52
3.4	Research design	54
	Research strategy	54
	Unit of analysis	55
	Data collection.....	58
	Data analysis.....	59
3.5	Conclusion.....	59
4	A CONTEXTUALIST INTERPRETATION OF STRATEGIC INFORMATION SYSTEMS SECURITY INITIATIVES	61
4.1	Introduction	61
4.2	Information Technology Agency	61
	Context	63
	Content	74
	Process	91
4.3	Department of Transportation	100
	Context	100

Content	107
Process	111
4.4 Discussion	118
4.5 Conclusion	120
5 DEVELOPMENT OF STRATEGIC INFORMATION SYSTEMS	
SECURITY INITIATIVES AT INFORMATION TECHNOLOGY	
AGENCY	121
5.1 Introduction	121
5.2 Bourdieu's cultural theory	122
5.3 Constructing the field map	126
Understanding position of the security department	127
Doxa	137
Characteristics of fields	143
Summary	150
5.4 Understanding habitus peculiarities	152
5.5 Appropriating power through forms of capital	163
Economic capital	163
Social capital	164
Cultural capital	167
Symbolic capital	169
The field of power	170
5.6 Strategizing about action	174

5.7 Attaining dominance through symbolic value.....	183
5.8 Discussion	195
5.9 Conclusion.....	202
6 IMPLEMENTATION OF STRATEGIC INFORMATION SYSTEMS	
SECURITY INITIATIVES AT DEPARTMENT OF	
TRANSPORTATION	204
6.1 Introduction	204
6.2 Gidden’s structuration theory	205
6.3 Shaping information systems security initiatives at Department of	
Transportation	209
Designing information systems security initiative.....	210
Instituting information systems security initiative.....	220
Discussion and summary	233
6.4 Social transformation at the Department of Transportation.....	236
Evaluating globalizing tendencies at DOT.....	238
Understanding self-identity at DOT.....	244
Discussion and summary	248
6.5 Discussion	251
6.6 Conclusion	258
7 INTERPRETING STRATEGIC INFORMATION SYSTEMS	
SECURITY INITIATIVES IN ORGANIZATIONS	260
7.1 Introduction	260

7.2 Understanding Schutz's concept of first-level constructs and second level constructs for social theory formation	261
7.3 Strategic information systems security initiatives at ITA.....	263
First-level findings	263
Second-level findings.....	268
7.4 Strategic information systems security initiatives at DOT.....	283
First-level findings	283
Second-level findings.....	288
7.5 Discussion	298
7.6 Conclusion	305
8 CONCLUSION	306
8.1 Recapitulating the doctrine.....	306
The nature of strategic information systems security	306
Shaping the strategic information systems security initiatives.....	308
The issue of technology governance	309
Summary of contributions of this research	312
8.2 Limitations and future research direction	315
Theoretical concerns	315
Methodological issues	317
References	320
Appendices	334
A. Information Technology Agency Case Study: Interviews Conducted	

.....	334
B. Department of Transportation: Interviews Conducted.....	337
C. Topic Guide.....	340
Vita.....	344

List of Tables

	Page
Table 2.1: Summary of formistic world-view.....	15
Table 2.2: Summary of mechanistic world-view.....	22
Table 2.3: Summary of organicistic world-view.....	30
Table 2.4: Summary of contextualistic world-view.....	35
Table 3.1: Analytic categories of contextualist security change.....	53
Table 3.2: Evaluative criteria for interpretive case study.....	56
Table 5.1: Position of ITA security department in various fields.....	134
Table 5.2: Characteristics of fields.....	143
Table 5.3: Types of capital.....	163
Table 5.4: Constitution of capital for field of power.....	172
Table 5.5: Types of strategy.....	175
Table 6.1: IS security implications from structurational analysis.....	252
Table 7.1: Unilateral control model for security development at ITA.....	270
Table 7.2: Unilateral control model for security implementation DOT.....	290
Table 7.3: Normative model for information systems security.....	299
Table 8.1: Evaluation of the dissertation.....	319

List of Figures

	Page
Figure 2.1: Scheme of world hypotheses.....	10
Figure 2.2: Information systems security literature.....	38
Figure 3.1: Contextualist model of strategic change.....	52
Figure 4.1: Organizational structure of the Information Technology Agency	70
Figure 4.2: IT security directorate of the Information Technology Agency	72
Figure 4.3: Organizational structure of the Department of Transportation.....	105
Figure 4.4: Information security department of the Department of Transportation.....	106
Figure 5.1: Bourdieu's cultural theory	123
Figure 5.2: Dominance through symbolic value.....	190
Figure 6.1: Structuration theory by Giddens	208
Figure 6.2: Model of strategic transformation	253
Figure 6.3: Model of strategic security organizational transformation	254
Figure 7.1: Theory-in-use model.....	269
Figure 8.1: Classification of theories and future research directions	316

Abstract

SHAPING STRATEGIC INFORMATION SYSTEMS SECURITY INITIATIVES IN ORGANIZATIONS

By Gurvirender Pal Singh Tejay, Ph.D.

A dissertation submitted in fulfillment of the requirements for the degree of Doctor of Philosophy in Business at Virginia Commonwealth University.

Virginia Commonwealth University, 2008

Major Director: Dr. Gurpreet S. Dhillon
Professor, Department of Information Systems

Strategic information systems security initiatives have seldom been successful. The increasing complexity of the business environment in which organizational security must be operationalized presents challenges. There has also been a problem with understanding the patterns of interactions among stakeholders that lead to instituting such an initiative. The overall aim of this research is to enhance understanding of the issues and concerns in shaping strategic information systems security initiative. To be successful, a proper undertaking of the content, context and process of the formulation and institutionalization of a security initiative is essential. It is also important to align the interconnections between these three key components. In conducting the argument, this dissertation analyzes information systems security initiatives in two large government organizations – Information Technology Agency and Department of

Transportation. The research methodology adopts an interpretive approach of inquiry. Findings from the case studies show that the strategic security initiative should be harmonious with the cultural continuity of an organization rather than significantly changing the existing opportunity and constraint structures. The development of security cultural resources like security policy may be used as a tool for propagating a secure view of the social world. For secure organizational transformation, one must consider the organizational security structure, knowledgeability of agents in perceiving secure organizational posture, and global security catalysts (such as establishing trust relations and security related institutional reflexivity). The inquiry indicates that strategic security change would be successful in an organization if developed and implemented in a brief yet quantum leap adopting an emergent security strategy in congruence with organizational security values.

CHAPTER 1

Introduction

1.1 Introduction

This research is concerned with strategic information systems security initiatives. In particular, the interest is in understanding how strategic security initiatives become instituted in an organization. The changes related to information systems security are seldom successful. These changes may relate to technical systems implementations or reconfigurations of business processes. The failure of such initiatives results in security gaps which can be detrimental to the well-being of an organization. It therefore becomes imperative to know what would make these security initiatives succeed in an organizational setting.

There is about a general lack of understanding regarding the patterns and relationships that have an impact on establishing strategic information systems security initiatives in an organization. This dissertation contends that strategic security initiatives need to be understood from a contextualist perspective. The overall aim of this research is to enhance understanding about the issues and concerns associated with instituting strategic information systems security initiatives in organizations. In pursuing this aim, this dissertation investigates the security related changes initiated in two large

organizations to address the dynamic requirements of the environment in which they operate.

The rest of this chapter describes the nature and scope of this research. Section 1.2 argues the importance of investigating the research problem. Section 1.3 outlines the scope of the research problem. Section 1.4 presents the definitions adopted in this research for the purposes of clarity and consistency of terms. Section 1.5 outlines the structure of chapters for the dissertation.

1.2. Nature of the Research

The need for strategic vision for information systems security is being felt by various organizations. According to David Burrill, Head of Group Security British American Tobacco, “what we're doing is lurching from challenge to challenge, from crisis to crisis” (as quoted in Scalet, 2005). “If you have no security plan, how will you know if you're doing it right? You will be reacting to every little thing that bumps in the night,” says Stan Gatewood, CISO of the University of Georgia (as quoted in Scalet, 2005). The emerging direction in information systems security practice is to consolidate various security functions. This trend in security practice has reaped initial success in some cases. But it might not work for every organization. “In the rapidly changing information security field...the strategic planning process is crucial if you want to get your organization out of crisis mode,” claims Sarah Scalet (Scalet, 2005). Organizations have embarked on rationalistic planning approaches that are prescriptive in nature to develop security programs, but these strategic efforts are not as effective as they could

be due to a lack of proper understanding of the problem at hand. In the absence of appropriate attention to the context, such efforts have a lower success rate.

The argument of this dissertation is that in order for strategic information systems security initiatives to be successful a proper understanding of the content, context and process of formulation and implementation is essential. The business world is comprised of events with disorder and change as its key features. To achieve a successful security program, the dynamics of security change under different contexts must be accounted for and properly understood. The contextual analysis of a security initiative involves investigation at various levels – issues at outer and inner context, historical influences and their interplay.

Based on the argument, this dissertation addresses the general research question about how to institute strategic information systems security change initiatives in an organization. The further sub research questions are:

- What aspects of information systems security goals, policies and programs should be included in a strategic information systems security initiative?
- How should strategic information systems security initiatives be formulated and implemented in an organization?
- Why and in what manner does the inner and outer environment of an organization impact the strategic information systems security initiative?

1.3 Scope of the Research

The purpose of this research is to develop theory. Information systems security research literature has witnessed limited efforts at theoretical development (Dhillon and Torkzadeh, 2006; Benbasat, 2001). The focus so far has been to address issues pertinent to security practitioners. These studies approach the security problem from a practical perspective and generally lack an appropriate theoretical underpinning. There are few research studies involving adequate empirical findings from a substantial research process. Further, there are a limited number of studies that investigate the security change efforts in its organizational setting. It is important to engage in theoretical debates to more substantively develop the field of information systems security.

In conducting the argument, the dissertation analyzes and studies the information systems security initiatives embarked upon in two large federated organizations – the Information Technology Agency and the Department of Transportation. The issues associated with the context, content and processes of the information security initiatives in the two case study organizations have consequences for the success of the strategic security programs in both these organizations.

Three classes of definitions are required to establish the conceptual boundaries of this research. For the purposes of this dissertation, an *information system* is considered as an aggregate of information handling activities at a technical, formal and informal level of an organization (Liebenau and Backhouse, 1990). This definition is also consistent with the view of an information system as advocated by Wetherbe and Whitehead (1977). *Information systems security* has traditionally been concerned with

securing the technical edifice. The definition adopted in this dissertation considers information systems security as minimizing risks arising because of inconsistent and incoherent behavior with respect to the information handling activities of organizations (Dhillon, 1995). In this dissertation, *strategic information systems security* is defined as a plan or pattern of actions to attain viability and effectiveness of an organization by securing information handling activities in the light of a changing critical environment. This definition is based on Quinn's and Mintzberg's definition of the strategic function. Quinn (1995) defines strategy as a pattern or plan that integrates an organization's major goals, policies, and action sequences into a cohesive whole. Mintzberg (1987) defined strategy as a plan, ploy, pattern, position, and perspective.

Strategy as plan is a consciously intended course of action, a guideline (or set of guidelines) to deal with a situation. Strategy as a ploy is a specific "maneuver" intended to outwit an opponent or competitor. Strategy is a pattern in stream of actions. Strategy as position is the mediating force or match between organization and environment between the internal and the external context. Strategy as perspective has its content consisting of an ingrained way of perceiving the world. (Mintzberg, 1987).

Many researchers have proposed definitions of the term strategy. In essence, these definitions actually capture Quinn's and Mintzberg's view of strategy in one form or another.

1.4 Structure of the Dissertation

This section presents an overview of the chapters in this dissertation. The research is structured in seven chapters. In this first chapter, the nature of the research problem was explicated and the scope of the research was described. Chapter two reviews the research literature in the field of information systems security. The aim of

literature evaluation is to position this research according to the philosophical underpinnings. The underlying argument is that security research needs to mature from mechanistic tendencies and ground itself in the contextualism paradigm.

Chapter three describes the research methodology. The philosophical assumptions of this research are discussed here. This chapter also provides the theoretical basis to conduct the research argument. It presents the research design with a particular mode of inquiry adopted for empirical analysis. Chapter four presents the contextualist interpretation of security initiatives in organizations. It provides an analysis of the Information Technology Agency and the Department of Transportation using the theoretical framework.

Chapter five presents the empirical findings from the Information Technology Agency case. The focus of this chapter is to evaluate the development of their strategic information systems security program. Chapter six presents the detailed findings from the Department of Transportation case and presents an analysis of the implementation of their strategic information systems security initiatives.

Chapter seven engages in a discussion based on the empirical findings from the two case studies. The findings are reviewed on the basis of theoretical underpinnings of the research. Finally, chapter eight presents the conclusions from this research.

CHAPTER 2

A Critical Review of Research in Information Systems Security

2.1 Introduction

The aim of this chapter is to review and understand the body of knowledge in information systems security. Such a review allows for an understanding of the philosophical underpinnings of extant work, which assists in positioning this research relative to the dominant paradigms of the field. The underlying argument of this chapter is that information systems security research needs to mature from mechanistic tendencies and ground itself in the contextualism paradigm. A similar endeavor is ongoing in information systems and prominent research works include Iivari (1991), Orlikowski and Baroudi (1991), Iivari et al. (1998), Dahlbom and Mathiassen (1993), Dhillon and Backhouse (2001).

The chapter is organized into eight sections. Following the introduction, section 2.2 presents the intellectual map that is used to understand the research literature. Section 2.3 discusses the formist view of information systems security. In this section, formism as a world hypothesis is described and used to analyze the literature. Section 2.4 presents the mechanist view of information systems security literature. Section 2.5

and 2.6 provides the contextualist and organicist views of the security literature respectively. Section 2.7 discusses the perspectives gained from employing world hypothesis as an intellectual tool to traverse the information systems security literature. Section 2.8 highlights the contribution of this chapter.

2.2 The Intellectual Map

Stephen C. Pepper was an American philosopher who was influenced by pragmatism. He primarily worked in the fields of ethics and aesthetics. His major research contributions have been to enhance understanding about the issues of social sources of knowledge, mind, logic, ethics and valuation. Pepper's work has influenced numerous disciplines including philosophy, psychology, education, management, mass communication, ethics, information systems, planning, ecological economics, and nursing. The most influential work by Pepper is the development of root-metaphor theory.

Pepper (1970) claims that our knowledge about the world can be reduced to four world hypotheses on the basis of the root-metaphor theory. Pepper argues that our knowledge about the world originates from common sense. There are two types of evidence – uncriticized and criticized. Every item of common sense should be critically scrutinized before accepting it. The appropriate way to do this is through corroboration. That is, in order to improve evidence we should find further evidence to corroborate it. There are two types of corroboration – multiplicative and structural. The former is the corroboration of man with man while the latter is corroboration of fact with fact.

In multiplicative corroboration, we confirm the repetition of the identical item of evidence in different occurrences. The facts are in the form of data which is collected through observation. The data so collected is loaded with interpretation. The refined data can be empirical or logical in nature. In structural corroboration, qualitatively different items of evidence converge in support of a single item. This type of corroboration depends upon a theory or hypothesis that connects different facts or items of evidence. In essence, it is the theory or hypothesis which is corroborated. The facts are in the form of *danda* which is captured through the hypothesis. *Danda* is a name given to evidence which has been refined through structural corroboration.

A theory or hypothesis is a structure which does not involve any evidence. Evidences for the hypothesis refer to various items that are not organized according to any structure. A structurally corroborated hypothesis can be refined in terms of precision or scope. An ideal hypothesis would have unlimited scope. Such a hypothesis is a world hypothesis. It is a legitimate cognitive source of prescription. The criteria for the determination of cognitive validity involves the specific theories of truth, perception, reason and scientific method that are associated with a particular world hypothesis. A number of world hypotheses have been proposed in the research literature which can be reduced by employing the root-metaphor theory. This theory is a descriptive summary of the trends of structural corroboration. The application of root-metaphor theory to the available world hypotheses provides us with four basic world theories that “are derived from certain masses of empirical evidence, originating in

common sense, which become cognitively refined and may be codified into sets of categories that hang together” (Pepper, 1970).

The four basic concrete standards of judgment and evaluation are formism, mechanism, contextualism and organicism (figure 2.1). These four world theories have the highest available degree of structural corroboration. These world theories are autonomous and have the same degree of adequacy so that they can not be the judge of one another. The guiding principles for the application of these theories are rational clarity in theory and reasonable eclecticism in practice. In terms of the knowledge about a particular subject,

...there are four well-corroborated alternative world theories about the subject which describes it in detail thus, thus, thus and thus. The post-rational eclecticism consists simply in holding these four theories in suspended judgment as constituting the sum of our knowledge on the subject. (Pepper, 1970)

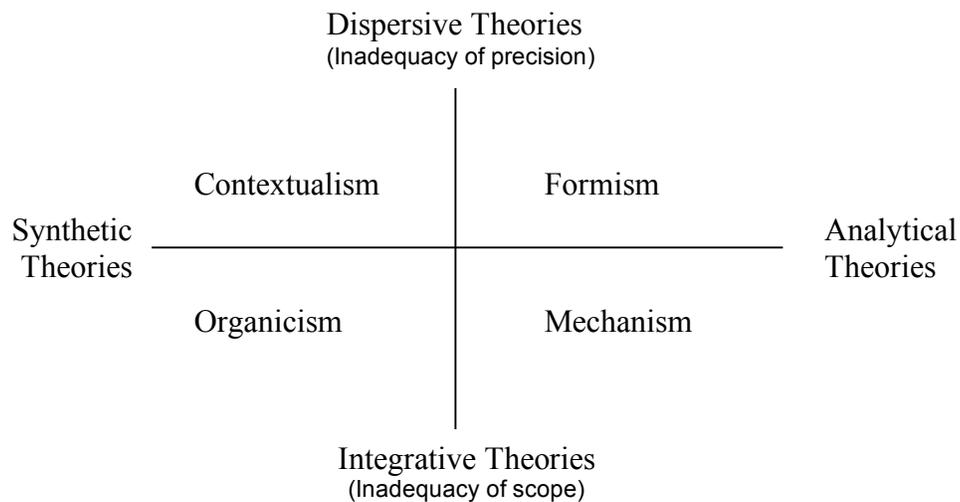


Figure 2.1: Scheme of world hypotheses

The four world theories organize themselves into analytical and synthetic theories, and further into dispersive and integrative theories. The main difference

between an analytical and synthetic theory is in terms of the basic facts. The basic facts of the analytical theories lie in the nature of elements or factors. As such, the synthesis of facts is derivative. The basic facts of the synthetic theories lie in the complexes or contexts. As such, the analysis of facts is derivative. Formism and mechanism are the analytical theories while contextualism and organicism constitute synthetic theories.

The main difference between a dispersive and an integrative theory is in the analysis of facts. In dispersive theories, facts are taken one by one from the original source and are interpreted as they arise or become evident. Formism and contextualism belong to this category of theories. For these theories, the universe is a multitude of facts that are loosely scattered, not determinative. The cosmos is not highly systematic. The idea of pure chance or unpredictability is consistent with these theories. Dispersive theories are threatened by indeterminateness or lack of precision. In formism, the problem of precision increases with added information about a “fact.” Here, the facts of determinate order are real while facts of disorder are unreal. For contextualism, the more we know about a “fact” the more determinate the description. Any fact is real for contextualism.

In integrative theories, the analysis of facts is treated integratively. The world appears as a cosmos where facts occur in a determinate order, and where, if enough were known, the facts could be predicted or described. Consequently, unpredictability or cosmic chance is inconsistent with these theories. The aim for integrative theories is to get everything into one determinate order. Integrative theories are threatened by the lack of scope.

The dispersive theories view integrative theories as profiting on human propensities to rationalization and sublimation. The integrative theories consider dispersive theories to be profiting on human ignorance. According to Pepper (1970), “mechanism is the stronger analytical and integrative theory, while contextualism is the stronger synthetic and dispersive theory.”

2.3 Research in Information Systems Security

This section classifies research in information system security. It first describes the world hypotheses and then systematically places the security literature research within each world-view. The methodology adopted to conduct the literature review is provided in Appendix A. Other researchers (Payne, 1975; Hayes et al., 1988) have similarly used the intellectual map provided by Pepper (1970) to understand the body of literature of the respective fields.

2.3.1 Formism as world hypothesis

There are two types of formism – immanent and transcendent formism. The immanent formism deals with the naturally occurring things, while transcendent formism covers artificially created or man-made products. The root metaphor of immanent formism is similarity. It implies the simple perception of similar things. For example, blades of grass, leaves on a tree. According to Pepper (1970), “immanent formism describes the experience of two exactly similar objects minutely, and accepts the results of this description.” Characters, particulars and participation are three

categories of immanent formism which can be considered as perception aspects of any event or object. Character refers to the characterizing entities, quality and relation of a given object. Particular refers to the individual manifestation. Its only characteristic is difference. Participation is the tie between characters and particulars to produce an object. It is particularization of character or characterization of a particular. Ties are categorical relations which cannot be characters. A given object may have a number of different characters that may occur in a number of different particulars. A class is a collection of particulars which participate in one or more characters. It is neither a character, nor a particular, nor participation, but an actual working or specific operation of three immanent categories in world. An organization of classes is called a classification.

It proceeds from more general to less general. That is, from classes with smallest number of characters and largest number of particulars to those with largest number of characters and smallest number of particulars. (Pepper, 1970)

The root metaphor of transcendent formism is plan and material. For example, develop objects according to the same plan or for the same reason. The objects are developed keeping in mind the limitations of the material. Transcendent formism has three categories – norms, matter for exemplification of the norm, and a principle of exemplification, which materializes the norms. There are laws of nature that are norms and regulate occurrences of nature.

Both immanent and transcendent formism recognize a category of forms, a category of the appearance of these forms in nature, and a category of the connection between first and second categories. The amalgamation of the categories of these two

forms of formism involve two important terms – existence and subsistence. Existence is the field of basic particulars, while subsistence is the field of basic characters. The categories can be merged as follows: forms consisting of characters and norms which may have second-degree participations with one another, basic particulars, and first-degree participations or exemplifications.

For a formist, all concrete existences do participate in the physical laws of space and time. That is, all characters appear in the form of time and space. A formist explains causality as a result of the participation of patterns, norms and laws in basic particulars through the forms of time and space. Causality is the determination of the characters of certain basic particulars by a law which is set in motion by the characters of other basic particulars which participate in that law. A law is a form. Norms are laws determining the concrete course of existence. In formism, systematic organization of facts is not assumed.

In formism, truth is the degree of similarity which a description has to its object of reference. There are two kinds of truth – historical and scientific (table 2.1). Historical truth refers to existence and describes the qualities and relations of particular events. Scientific truth refers to subsistence and describes the norms and laws. These descriptions can be of empirical uniformities or of natural laws. The former are considered as half-truths whereas the latter are considered full truths. Epistemologically, for the knower the world is known directly. In formism, laws of nature are discrete and separate from each other. There is no single integrated system. For formism, there is reality of forms distinct from the reality of particulars.

Table 2.1: Summary of formistic world-view

Root (Ontology)	Similarity; plan and material		
Epistemology	World is known directly		
Aim of Enquiry	To classify		
Theory of Truth	Degree of similarity which a description has to its object of reference		
	Types of Truth	Refers to	Description of
	Historical	Existence (basic of particulars)	Qualities and relation of particular events
	Scientific	Subsistence (basic of characters)	Norms and Laws
Inadequacy	Precision		
Logic	Similarity		
Categories	1. Forms		
	2. appearance of forms in nature		
	3. connection between first & second category		

Information systems security literature

A common approach in the formistic world view is to classify research literature according to the similarity of elements. It is a logical approach to identify gaps and problematic areas with respect to prevalent theories and approaches. Dhillon & Backhouse (2001) used the Burrell and Morgan framework as an intellectual map to analyze the socio-philosophical concerns in various information systems security approaches. It is important to understand the theoretical concepts that form the basis of a methodological approach. The prevalent literature in information systems security has used the formistic view to study areas of concern like threats, computer abuse and planning.

Loch et al. (1992) investigated management information systems (MIS) executives' concerns about different types of threats. This research study presented a framework for the source and perpetrator of threats to information systems security. The analysis indicated a gap between the use of technology and an understanding of the

security implications inherent in its use. The focus of the study was to classify threats to microcomputers, mainframes, and networks. Likewise, Ryan and Bordoloi (1997) concentrated on the security threats in mainframe and client/server environments. This research paper addresses the commensurability of security measures against the seriousness of potential threats in the two environments. The authors argue for a proactive approach to address security exposures to an organization. In building upon the proactive assertion, Jung et al. (2001) argued the need to identify specific threats before designing a secure system and they broadened their focus to examine security threats across four industries - manufacturing, banking/financial, research institution/university, and distribution/service. The threats are catalogued as interruption, interception, modification, and fabrication. These threats are then investigated against five types of security services - authentication, access control, data confidentiality, data integrity, non-repudiation.

The possibility of occurrence of threats results in significant risks to information systems. Boockholdt (1989) provides a classification of risks associated with linking of personal computers to a corporate mainframe computer. The study examines the impact of the link on computer security and data integrity and identifies critical guidelines to control such risks. In another research paper (Boockholdt, 1987), the author addresses the impact of microcomputers on information systems integrity and security. The study is formistic in nature as it outlines the impact not the causal connection, that is, does not correlate parts to security. Risks to an information system also arise from the use (or misuse) of passwords (Zviran and Haga, 1999). These authors list the core

characteristics and associations of user-generated passwords. This research study addresses the gap in evaluating the characteristics of real-life passwords. To address the inadequacy of security in organizations, Straub and Welke (1998) employed the general deterrence theory to argue for the formalization of a specific aspect of security. The authors contend that security managers fail to cope effectively with systems risks because they lack awareness of the full range of security controls available for implementation. The paper classifies security risk control measures as a security program which includes use of a security risk planning model, education or training in security awareness, and countermeasure matrix analysis. A checklist in the form of guidelines is also provided to help managers cope with risk.

The abuse of information systems is a critical problem for organizations. In an earlier definition, Kling (1980) defines computer abuse as unauthorized, deliberate and internally recognizable misuse of assets of information systems by individuals. The concern has varied from disciplining such a behavior to monitoring employees who use computers. Straub and Nance (1990) group various organizational responses to the problem of computer abuse, including discovery of abuse incidents and discipline of perpetrators. The authors formulate an approach to security administration in terms of security effort allocations and disciplinary actions. The case for security administration is supported by Ariss (2002) who argues for effective supervision as a business necessity. The research paper classifies the advantages and disadvantages associated with computerized monitoring at the workplace. However, the author warns against

excessive computer monitoring since it may be regarded by employees as unethical and prove to be economical destructive.

The problem of computer abuse has also led to the emergence of privacy issues. Turn (1987) presents an overview of the basic issues for privacy protection and implementation requirements. The author examined problems that arise in extending privacy protection to international data processing systems. Protection of privacy is a major concern for consumers of information systems. Smith et al. (1996) categorizes information privacy practices of the organizations. The paper identifies and measures the primary dimensions of individuals' concerns about organizational information privacy practices. The authors argue that the researchers cannot credibly test explanatory theories regarding causal links between practices, individuals' perceptions, and societal response in the absence of a validated instrument. The aim of the paper is not to check for causality relationships and does not provide a causal model.

Summary

The formist view informs us about the similarity of forms inherent in the nature of information systems security. Researchers have investigated threats, computer abuse and planning aspects of security. In doing so, various classification schemes have been developed and presented to increase our understanding of information systems security. For threats, researchers have proposed typologies and categories to understand the nature of threats. The issues associated with computer abuse have been categorized and grouped together to provide descriptions of uniformities. The formistic view of behavior

as immanent in the element because it is a member of a particular class has been usefully employed to investigate security planning. Checklists, guidelines and matrices to control the critical factors of the planning process are based on the consideration of class member characteristics.

2.3.2 Mechanism as world hypothesis

The root metaphor of mechanism is machine. A machine is composed of discrete parts related to each other in a systematic way. Each part exists independently. In a machine, a force is exerted or transmitted through the system to produce predictable outcomes. There are two types of mechanism – discrete and consolidated. Discrete mechanism considers structural features of nature as loosely or externally related. It emphasizes independence in the world. This leads to accident and necessity.

Accidental comes from the conception of the independence of details, and the necessary from the inevitability of the event's being just what it is since there is no reason to be found for it being anything different. (Pepper, 1970)

Traditional discrete mechanism involves theory of elementary particles distributed in space and time.

Consolidated mechanism considers details to be involved and determine one another. There is no accident. There are no laws in consolidated mechanism, only structural modifications of spatiotemporal field. There are no primary qualities as these are resolved into field laws, which are themselves resolved into the structure of the field. In consolidated mechanism, only a particular exists namely spatiotemporal-gravitational-electromagnetic field. This type of mechanism lacks in scope.

Mechanism consists of primary and secondary categories. The primary category includes the field of location, primary qualities, and primary laws. The field of location defines existence and reality. The fundamental particulars are time and space. Primary qualities are concerned with the properties of location in the field and differentiating properties. Laws holding for configurations of primary qualities in the field are the primary laws. There is confidence in precisely determined laws. The universe is considered to be completely mechanized and internally determined.

Secondary categories consist of secondary qualities, a principle for connecting secondary qualities with the first three primary or effective categories, and secondary laws. Secondary qualities involve characters of human perception. These are irreducible characters of the world which are not identifiable with primary categories. In terms of connecting principle, three main theories have been proposed - identity, causation and correlation. Correlation is the only promising one and is signified with emergence. Emergence signalizes correlated appearance. Secondary laws are the laws for regularities among secondary qualities.

Mechanism considers immediate evidence to be of secondary qualities which are private to each individual organism. As such, mechanism knowledge of the external world is symbolic and inferential. The theory of truth of mechanism is the causal theory of truth. This theory implies a system of causal connections which holds between an environmental stimulus and response of an organism. Truth thus becomes a name for physiological attitudes which are in adjustment with the environment of an organism. Error arises from lack of adjustment of body.

The older theory of truth is the theory of correspondence which considers truth as correspondence between visual images and external facts. Here idea and object are being compared. This theory was replaced by symbolic theory of correspondence. In this theory, an idea is a group of symbols in a sentence or formula. Truth then equates to symbols corresponding with features of an object and symbolized relation among symbols with relation among objects. The inherent deficiencies of this theory led to operational theory of truth. This theory considers truth of a formula as its workability. In other words, this theory rejects the importance of correspondence and emphasizes the predictive power of sentence or formula to produce expected results.

The inadequacy of this hypothesis results from the gap between primary and secondary categories. In mechanism, causal connection is excluded and correlation is all that remains. The causal adjustment theory of truth covers this gap but the concept of correlation has implications for formistic similarity. In mechanism the goal is to discover the parts and relations among the parts of existent machine (table 2.2). The part is basic and the whole is a synthesis of parts. Mechanists seek to discover the true nature of a given event by specifying what kind of part it really is and by placing it properly in the machine. This goal is aided by apriori model or theory. This hypothesis is resonant with hypothetico-deductive research methodology.

Table 2.2: Summary of mechanistic world-view

Root (Ontology)	Machine	A machine is composed of discrete parts related to each other in a systematic way. Each part exists independently.	
Epistemology	Symbolic & Inferential	Knowledge of external world is symbolic and inferential. Immediate evidence is of secondary qualities which are private to each individual organism.	
Aim of Enquiry	To correlate		
Theory of Truth	Causal Theory of adjustment	A system of causal connections which holds between an environmental stimulus and response of an organism.	
Inadequacy	Scope	Gap between primary and secondary categories.	
Logic	Causality		
Categories	Primary	1. Field of location	defines existence and reality. The fundamental particulars are time and space.
		2. Primary qualities	properties of location in the field, and differentiating properties
		3. Primary laws	Laws holding for configurations of primary qualities in the field.
		There is confidence in precisely determined laws. The universe is considered to be completely mechanized and internally determined.	
	Secondary	1. Secondary qualities	Involve characters of human perception. These are irreducible characters of the world.
		2. Principle for connecting secondary qualities	Three main theories: identity, causation and correlation.
		3. Secondary laws	Laws for regularities among secondary qualities.

Information systems security literature

The research literature that uses the mechanistic approach to information systems security is discussed in this section. Risk management has been the traditional approach to address information systems security issues, in addition to checklists (Dhillon and Backhouse, 2001). Kotulic and Clark (2004) point to the lack of empirical research in the area of security risk management to justify the importance of their study. The authors provide a conceptual model for security risk management program effectiveness based on a firm-level study. Their study is based on the assumption of causality addressing only a few factors to achieve an effective security risk management program. This study provides an interesting twist as it provides details on how the

validation of their research model was unsuccessful. The authors argue that information security research is one of the most intrusive types of organization research. As such, the authors do not propose the use of mass mailings of survey instruments when attempting to collect sensitive data. However, Sun et al. (2006) developed a theoretically grounded methodology for risk assessment of information systems security. Their method is based upon evidential reasoning approach of the theory of belief functions. It defines security risk as the plausibility of security failures.

The main objective of technical security is to protect corporate data. This objective is the motivation for the research study by Murray (1979). The author argues for the use of cryptographic transformations as an effective data security technique. The data stored on a single computer needs to be protected; however such an approach does not capture the reality of data use. The data should be secured in a distributed system also. Bussolati and Martella (1981) argue that the security architecture should reflect the logical architecture of the distributed system. The authors are concerned with the security data management in a distributed data base of aggregated type. Further, the existing data should be evaluated in terms of security to prevent vulnerabilities. Sarathy and Muralidhar (2002) argue for the importance of determining the extent to which confidential attributes may be exposed to attacks. As such, the ability to evaluate the extent of disclosure for such data is significant. In particular, the research study develops a methodology using canonical correlation analysis for evaluating inferential value disclosure of either individual or linear combinations of confidential numerical attributes by snoopers. Another approach to the data integrity issue is to address

strategic information manipulation. Biros et al. (2002) conduct a research study with causal underpinnings that by inducing sensitivity to deception we would be able to improve decision-making performance. The aim of this study is to examine the effects of manipulated data on professionals' task-related decision behaviors: deception detection, false alarms, and task accuracy. The authors argue that professionals must be sensitive to the threat of deception if users are to improve their ability to detect deceptive data. An interesting approach to ensure data security is the proposal to use electronic signatures. Gupta et al. (2004) question the cost savings and security associated with electronic signatures across business activities. The authors argue that the benefit of digital signatures lies in the potential improvement of stepwise sign-off processes including negotiation and contract/document generation. To enable different business processes, the documents have to be explicitly managed as a collection of entities with multiple ownerships. The authors highlight the need for a secure and authentication-based automated document management and contract negotiation system.

Access control issues address information systems security from a technical viewpoint. Roos (1981) was an early proponent for the socio-organizational perspective by highlighting the importance of end user responsibility. The aim of the research study by Roos (1981) is to understand confidentiality of information. The author argues that data sharing control is weakened with any departure from strictly preventive controls. End user responsibility for information control is defined as the relationship between organization structure, the supporting information systems and the confidentiality issue.

In terms of technical access control approaches, the security for multilevel and distributed systems has been of chief concern. Thuraisingham (1993) addressed multilevel security issues for information retrieval database management systems. In a later study (Thuraisingham, 1995), the author addressed security issues for linking the conceptual nodes in the context of hypermedia-based information retrieval systems. The paper provides direction for designing systems that support the data processing requirement of next generation systems. Yiu et al. (2006) discusses the issue of sharing access rights and claim they are critical to designing information systems. Their research addressed sharing of encrypted documents and delegating the access rights of encrypted documents. The research problem can be reduced to that of storing confidential documents in a system. The authors argue that an access control list and session key symmetric encryption should be components of the solution system.

Unauthorized access to an organization's information system can be effectively checked by intrusion detection systems. Cavusoglu et al. (2005), however, argue for a rigorous assessment of the value of intrusion detection systems in IT security architecture. In this paper, the IT security problem is modeled as a game between a firm and a hacker where the former attempts to minimize loss from a security breach and the latter aims to compromise the information systems of that firm. It is assumed that the model parameters were common knowledge to the firm and users. The analysis indicates that the value of an intrusion detection system lies in increased deterrence, which is enabled by improved detection. However, the firm would only be able to

realize this value potential if the firm optimally configures the IDS based on the hacking environment.

The inadequacy of technical approaches in addressing security issues in organizations has led some researchers to study behavioral aspects as well. Goodhue and Straub (1991) argue for a better understanding of security concerns focusing on users' perceptions about the security of their systems. A user's concern about security is considered to be a function of industry risk, company actions, and individual awareness. Frank et al. (1991) believe an understanding of security-related behavior of personal computer users in organizations is important for controlling behavioral security. The behavior and attitudes of users' towards backup, documentation, data storage, and file access practices was examined in their research paper. The analysis indicates that user knowledge and informal department norms are significantly related to security-related behavior. The underlying assumption is that of correlation in terms of variables that impact security-related behavior of users. Harrington (1996) also examined the intentions of information systems employees. The author uses vignettes to understand the casual connection between codes of ethics and computer abuse judgments. Another area of concern has been the creation of passwords for system access. Adams and Chang (1993) employ the theory of the search of associative memory as the theoretical lens to anticipate what subjects will choose for passwords or personal identification numbers (PIN). The authors argue that security can be improved by providing users with a keypad (or an image of it) while creating the passwords. The causal nature of the research study underlies the problem of how passwords can be made more secure.

Corporate managers need to be security prudent in their decisions pertaining to organizational activities. Even decisions involving software choices require the keen involvement of managers who are well versed in IT security. For instance, the effectiveness of open source software in terms of security issues has been evaluated by Payne (2002). The research study empirically assesses the relationship between open source code and security against the dimensions of confidentiality, integrity, availability and audit. The findings indicate that open source software is not intrinsically more secure than proprietary code. Post and Kagan (2000) examined organizational responses to the threat of computer viruses. The three basic sets of tools considered in this study to minimize the threat of virus are management policies, anti-virus software, and backup procedures. The authors highlight the importance of identifying the trade-offs between different tools. The study is mechanistic in nature as it correlates the effect of various tools to combat virus threat. The critical nature of policies for security has been established by Katos and Adams (2005). The authors argue for the need to adopt appropriate and consistent policies to satisfy privacy rules and security concerns. The theory of information richness is used to develop the foundation for privacy and security policies metrics.

In recent times, alliances have been suggested as an effective method to ensure organizational security. Gal-Or and Ghose (2005) investigate the implications of sharing security information and the impact of investments in security technologies. The authors assume a rather simplistic model of the world where the market consists of two firms producing a differentiated product in a two-stage non-cooperative game. The

approach followed is that of economic modeling based on the field of industrial organization. The authors argue that economic issues would impact achievement of the goal. The findings indicate that security technology investments and security information sharing are strategic complements in equilibrium. Further, the sharing alliances would yield greater benefits in competitive industries.

Summary

The mechanist view informs us about the casual connections in the nature of information systems security. The universal structure of information systems security is analytically investigated to identify the components in order to explain its true nature. Models, relations, linkages and functions have been predominantly used by security researchers to establish correlation among different components considered critical to attain effective security. Various data security and risk management methodologies are based on the insight that behavior of the whole is deliverable from the behavior of the parts. Analytic modeling explores the intricacies of access control mechanisms and information sharing based on the assumption that driving force of some sort is necessary in any operation of information systems security.

2.3.3 Organicism as world hypothesis

The root metaphor of organicism is organism or integration. It is the process of organic development where integration in the process is of interest not duration. In organic systems, change is given and stability has to be explained. The operation of

rules of change needs to be explained, assuming that change occurs according to these rules. The whole is basic, and parts are meaningless except in the context of the whole. Organicism approaches every actual event in the world as concealed organic process (historic process).

The categories of organicism consist, on one hand, in noting the steps involved in the organic process, and, on the other hand, in noting the principal features in the organic structure ultimately achieved or realized. There are seven categories, which are the features of any organic or integrative process and its achievement. 1) Fragments of experience which appear with, 2) nexuses or connections or implications, which spontaneously lead as a result of the aggravation of, 3) contradictions, gaps, oppositions, or counteractions to resolution in, 4) an organic whole, which is found to have been, 5) implicit in the fragments, and to 6) transcend the previous contradictions by means of a coherent totality, which 7) economizes, saves, preserves all the original fragments of experience without any loss. Categories 1-4 are the progressive categories which deal with appearance. Ideal categories deal with reality and consist categories 4-7.

A fact is referred by a judgment which is a fragment in itself. A judgment is a fragment and its nexus. The truth of a judgment consists in fragment's finding, through its nexus, a whole in which it is free from contradictions. The formal expression of judgment is always in terms of verbal or mathematical symbols. It is not essentially the sentence that is true, but what the sentence means, that is, the judgment. The degree of truth improves with an increased integration of facts. The criteria of truth are

inclusiveness, determinateness, and organicity. This theory of truth is known as coherence theory. Coherence is the positive organic relatedness of material facts. For organicism, we cannot know the whole truth until absolute is attained. Absolute is fact itself and is completely organic. Epistemologically, organicism adopts constructivism. For organicism, the knower actively contrues the world.

Organicism has a limitation of inadequacy of scope (table 2.3). Progressive categories are required to give scope to organicism but progressive categories involve time, change, and finitude. Time, change, and finitude cannot be true as only the absolute is true and in the absolute there is no time, change or finitude. This is the contradiction.

Table 2.3: Summary of organicistic world-view

Root (Ontology)	Organism or integration	The process of organic development where integration in the process is of interest not duration.
Epistemology	Constructivism	The knower actively contrues the world.
Aim of Enquiry	To integrate	
Theory of Truth	Coherence theory	The positive organic relatedness of material facts
	Degree of truth	Improves with an increased integration of facts
	Criteria of truth	Inclusiveness, determinateness, organicity
Inadequacy	Scope	Progressive categories involve time, change, and finitude. Time, change, and finitude cannot be true as only the absolute is true and in the absolute there is no time, change and finitude.
Logic	Structure	
Categories	Progressive (deals with appearance)	1. Fragments of experience which appear with,
		2. nexuses or connections or implications, which spontaneously lead as a result of the aggravation of,
		3. contradictions, gaps, oppositions, or counteractions to resolution in,
		4. an organic whole, which is found to have been
	Ideal (deals with reality)	5. implicit in the fragments, and to
		6. transcend the previous contradictions by means of a coherent totality, which
		7. economizes, saves, preserves all the original fragments of experience without any loss.

Information systems security literature

The research literature employing the organistic view of information systems security is discussed in this section. Information systems security is actually a corporate governance responsibility (Posthumus and von Solms, 2004). The authors argue that appropriate security governance would lead to an increase in overall productivity of the organization. The paper develops an information security governance framework that integrates information security into corporate governance. Voicing similar concerns, von Solms (2005) argue for implementing comprehensive and standardized information security governance environments. The research paper examines the complementary nature of COBIT and ISO 17799 as reference frameworks for information security governance. However, any model for information security governance must emphasize or integrate the control aspects of corporate governance (von Solms and von Solms, 2006). The authors propose a security governance framework which is based on the direct-control cycle.

Since the security requirements differ from one organization to another, the generic information security standards are ill equipped to serve as a basis for security policy development (Baskerville and Siponen, 2002). As such, the authors address the current requirement for information security policy formulation to be federated and emergent. The research paper proposes a meta-policy that addresses the concerns of security policy formulation, implementation, enforcement and validation. A meta-policy could take into account critical organizational requirements and would lead to an integration of security throughout the process of information systems development and

management. The position of integrating security into higher information systems processes is also supported by Doherty and Fulford (2006) who investigate the relationship between strategic information systems planning and information security management. The authors argue that a strategic information systems plan is a critical prerequisite for information security policy formulation and the two should be carefully aligned. In a specific narrow context, Morin and Pawlak (2006) encourage debate at the policy management level to discuss the strategic dimension of digital rights management. The authors propose a framework for studying, analyzing and defining corporate policy management towards its partial digital instrumentation. The assertion is that enterprise information systems will have to factor in persistent protection, governed usage and managed content in the future which represents a major challenge.

The absence of international criteria or standards poses problems for the management of information systems security (von Solms et al., 1994). The authors argue that information security policy, risk analysis, risk management, contingency planning and disaster recovery are all interrelated in some way. Therefore, any evaluation of information security should be conducted according to internationally accepted criteria. A model for information systems security management is proposed.

Summary

The organicist view informs us about the structural characteristics inherent in the nature of information systems security. The significance in the integration of the process is highlighted by security researchers who propose various governance and

policy approaches. Such an approach contends that components cannot be explained without reference to the whole structure of information systems security. The interrelatedness of various components of security is critical for an international standard and emphasizes the meaninglessness of parts except in the context of the whole.

2.3.4 Contextualism as world hypothesis

The root metaphor of contextualism is historic event. A historic event is an act in and with its setting, and an act in its context. Disorder and change are the categorical features of contextualism. Contextualism believes in a given event and direct verification. It emphasizes the changing present event (changed into something novel). The contextualistic categories are change and novelty which are exhibited in quality and texture. For contextualism, the entire world is comprised of events and every given event has quality and texture.

Quality of a given event is its intuited wholeness or total character. It is the experienced nature of an event. Quality involves spread, change and fusion. Spread is the feeling of future or history. It is characterized by specious present which is the basic structure of all events or facts. Change goes on continuously and never stops. It is the categorical feature of all events. As such, for contextualism the whole world is continuously changing. Fusion involves the integration of textural details of a given event. It is an agency of qualitative simplification and organization.

Texture deals with the details and relations of an act that make up its quality. It is made up of strands and it lies in a context. Quality consists of strand, context and references. Strand is whatever directly contributes to quality of texture. It is the interconnection among details of an act. Context is whatever indirectly contributes to quality of texture. It is the interconnections among strands. References are strands more intimately considered. It is temporal relation or interconnections between details. References maybe linear, convergent, blocking or instrumental.

In contextualism, actual structure of an event is ultimately determined by its qualitative structure. For contextualistic theory of analysis, there is no final or complete analysis of anything. There is no top or bottom in contextualistic world. The support of every texture lies in its context. There is no cosmological mode of analysis that guarantees the whole truth or an arrival at the ultimate nature of things. One does not need to hunt for truth, as every present event gives it as fully as it can be given. All one has to do to get at the sort of thing the world is, is to realize, intuit, and get the quality of whatever happens to be going on. Significance lies in some purpose we are pursuing. An analysis is always for some purpose.

The theory of truth for contextualism is the operational theory of truth. It is truth in terms of action, of actual events having references which lead to satisfactions in other events. The question of truth arises when a strand is blocked. That is, a problem arises and we seek a solution to the problem. We analyze the situation in search of a hypothesis that will lead us to a solution of problem. This analysis consists in following strands of a blocking condition within the context of a blocked strand. This leads to

various relational schemes. Truth is the result of an instrumental texture which removes a blocking and integrates a terminal texture. Contextualism is threatened with evidences for permanent structures in nature.

There are three distinct specifications of theory of truth: successful working, verified hypothesis, and qualitative confirmation (table 2.4). In successful working, truth is utility or successful functioning. Successful action is the true one. This specification implies that a hypothesis can never be successful when it is framed, nor can success ever be hypothetical when it comes. The problem arises as the hypothesis is excluded from truth. For a verified hypothesis, truth is in verification. It is not the successful act that is true, but the hypothesis that leads to the successful act.

Table 2.4: Summary of contextualistic world-view

Root (Ontology)	Historic event	An act in and with its setting, act in its context	
Epistemology	Belief in given event and direct verification.		
Aim of Enquiry	To attend		
Theory of Truth	Operational theory of truth	Truth in terms of action, of actual events having references which lead to satisfactions in other events.	
Inadequacy	Precision		
Logic	Distinction		
Categories	Quality	Quality of a given event is its intuited wholeness or total characters.	
		Spread	The feeling of futurity or pastness. It is characterized by specious present which is the basic structure of all events.
		Change	Change goes on continuously and never stops. All world is continuously changing.
		Fusion	The integration of textural details of a given event. It is an agency of qualitative simplification and organization.
	Texture	Texture deals with the details and relations of an act that make up its quality.	
		Strand	whatever directly contributes to quality of texture. It is the interconnection among details of an act
		Context	whatever indirectly contributes to quality of texture. It is the interconnections among strands.
		References	strands more intimately considered. It is temporal relation or interconnections between details.

Truth is the relation between a hypothesis and its eventuality rather than the quality of an act as successful or unsuccessful. In total, there are three articulations: the

formulation of a symbolic texture (hypothesis), a following out of symbolic references (operations), and a satisfaction or blocking of these references (verification proper). A hypothesis is true if satisfaction is achieved in the verification. For qualitative confirmation theory, truth is a relation dependent upon the act of verifying. A true hypothesis coheres and corresponds with the event that verifies it. “Qualitative confirmation” theory suggests that the body of hypotheses possessed by science and philosophy gives us a considerable amount of insight into the structure of nature. Contextualism is very definite about the present event and premonitions it gives of neighboring events, but less and less definite about the wider structure of the world.

Information systems security literature

Backhouse et al. (2006) approach standards as instruments of power. The authors theorize about the power mechanisms required for a standard to evolve from an idea into an obligatory passage point for organizations and agencies. The argument is that power operates silently but relentlessly in the generation and institutionalization of a standard, and brings to light valuable insights into the social and political processes that form the core of standards setting work. It studies an event in its context. The argument is based on an underlying assumption that the institutionalization of a standard is initiated by exogenous contingencies in an organizational field. The authors criticize the economics approach in explaining development of a standard. They contend that the decisions about design and implementation of standards are not normally reached on the basis of a rational-logical process, but are instead constructed

through the constant realignment of interests among the actors involved. This research study uses the theory of circuits of power to reveal the power mechanisms that shape that realignment. It examines the interaction of external contingencies, powerful agents, resources, meaning and membership of relevant social and institutional groupings in generating successful political outcomes. Even though actors are key to the generation and adoption of standards in general, institutional factors, such as regulation and legislation, also play a fundamental role. The study underlines the part played by alliances and legitimacy in obtaining sufficient support for an emerging standard.

2.4 Discussion

The world hypotheses involving formism, mechanism, contextualism and organicism are four different ways to look at the world (Pepper, 1970). In this chapter, we used the four hypotheses to help us understand the body of knowledge developed so far in the field of information systems security. The respective world hypotheses provide us with an interesting and different approach to analyze and understand the world. In purist terms, mechanism and contextualism are considered to be the stronger among the other hypotheses (Pepper, 1970). However, this is not the view taken in this chapter. In analyzing the security research literature, it is argued that each of these hypotheses is critical for improving our understanding about the complex world of information systems security.

As discussed in the previous section, the formist view informs us about the similarity of forms inherent in the nature of information systems security. Various

classification schemes (Kling, 1980; Boochholdt, 1989; Turn, 1987; Loch et al., 1992; Straub & Welke, 1998) have been developed and presented to enhance our knowledge. The mechanist view informs us about the casual connections in the nature of information systems security. The universal structure of information systems security is analytically investigated to identify the components (Murray, 1979; Roos, 1981; Bussolati & Martella, 1981; Goodhue & Straub, 1991; Harrington, 1996; Payne, 2002; Cavusoglu et al., 2005; Sun et al., 2006) in order to explain its true nature. The organicist view informs us about the structural characteristics inherent in the nature of information systems security. The significance in the integration of the process (Baskerville & Siponen, 2002; Doherty & Fulford, 2006) and the importance of whole structure (von Solms et al., 1994; Posthumus & von Solms, 2004) has been emphasized. The contextualist view informs us about the distinctions in various events of information systems security. It is important to include context (Backhouse et al., 2006; Karyda et al., 2005) in the analysis of an act. The four corroborative alternative world theories, namely formistic, mechanistic, contextualistic and organicistic theory of security, constitute the sum of our knowledge on the subject of information systems security (figure 2.2).

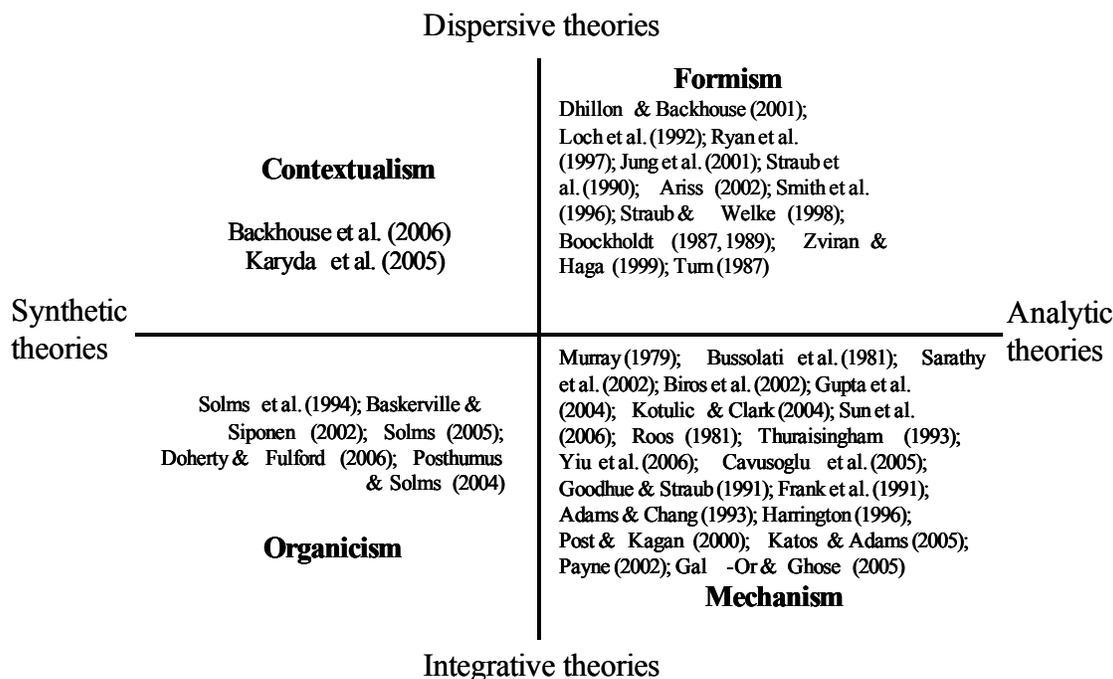


Figure 2.2: Information systems security literature

In studying information systems security, researchers have used analytic theories to understand the security problems. The basic facts of analytical theories lie in the nature of elements. Although such an approach is useful it is imperative for security researchers to examine the other end of the spectrum to obtain a complete picture. The increasing complexity of the security environment requires an understanding of the context in which any initiative is introduced. In order to be successful, security problems need to be studied from the position of synthetic theories. The basic facts of synthetic theories lie in the contexts or complexes. There is a dearth of security research employing a synthetic perspective of the world. The significance of research analysis lies in the research purpose that is being pursued. Such an analysis would provide rich

insights of the security aspects under consideration. In order to understand the nature of information systems security it is imperative to realize, intuit, and obtain the quality of the event of interest, which involves an act in and with its setting.

The analysis of the extant information systems security literature indicates that researchers have predominantly used analytic theories to understand the security problem. This is evident from figure 2.2 where the research studies depicted on the right of the vertical axis (dimension of analytic theory) significantly outnumber those on the left of the vertical axis (signifying dimension of synthetic theories). The focus of analytical theories lies in the nature of elements. In following this position, the dominant security research theme has been to find the factors or components that would impact overall organizational security. The mechanistic tendencies in information systems security research have also been noted by Dhillon & Backhouse (2001) and Dhillon and Torkzadeh (2006).

To improve the security posture of an organization it is imperative to realize, intuit, and get the quality of the event of interest, which involves an act in and with its setting (Pepper, 1970). At the same time, it is also important to understand the constituent, as well as, processual models for the implementation of a successful information systems security program. An eclectic approach to study the security problem is better than a static approach. The complexity of security problems can only be navigated successfully if we take into account the different positions of the dominant security paradigms. In other words, we need to investigate how the content and context of the security programs are linked together. The content comprising of security

objectives and security policy would interact with the security culture, security governance structure and the political context of an organization to generate possible changes that may or may not be aligned with the intended security goals of an organization. Similarly, we also need to understand how the link between context and process of security implementation can have an impact on the outcome of the security initiative. The study of these linkages would provide a richer understanding of the nature of information systems security problems.

A finding of the literature review is that a significant number of studies adopt an analytic theoretical position rather than a synthetic one, which reflects the maturity of information systems security as a discipline. During the early stages of development of a discipline, we are intrigued with the factors or elements and our tendency is to classify them so as to come to grips with the subject. This is the case with the discipline of information system. Several instances of early studies which were based on a formistic notion of similarity include: Senn (1978), Alter (1978), Swanson and Culnan (1978), Weiss (1980), Nolan and Weatherbe (1980), Colter (1984), Stabell (1987), Barki et al. (1988), Necco et al. (1987), Tan and Benbasat (1990), Baroudi (1991), Meyer and Curley (1991), Byrd and Zmud (1992), Goldstein and Storey (1992), Ein-Dor and Segev (1993), and Choudhury (1997). Next, we try to figure out the relationships between various factors. We seek the causal connections between various dependent and independent factors. In information systems, the research stream focused on user acceptance, in particular the technology acceptance model (Davis, 1989, Davis et al. 1989) can be seen as an instance of the proliferation of research imbued in mechanistic

tendencies. Few prominent studies conducting research in this area include: Mathieson (1991), Adams et al. (1992), Szajna (1994), Taylor and Todd (1995), Igarria et al. (1995), Chau (1996), Venkatesh and Davis (1996), Jackson et al. (1997), Gefen and Straub (1997), Igarria et al. (1997), Lucas and Spitler (1999), and Dishaw & Strong (1999). As the discipline matures, our focus of interest moves to the field where the factors interact. We become engrossed with the event of interest and explore our understanding of the complex setting. There are significant research studies in information systems that abide by the tenets of synthetic theories. These studies include research by Wijnhoven et al. (2006), Gao (2005), Wagner and Newell (2004), Irani et al. (2005), Nandhakumar et al. (2005), Wilson and Howcroft (2005), Liang and Xue (2004), Caldeira and Ward (2002), Avgerou (2001), Ang et al. (2001), Walsham and Sahay (1999), Barrett and Walsham (1999), Ward and Elvin (1999), Mao and Benbasat (1998), and Shanks (1997). However, there remains a lack of empirical security research employing this view of the world.

Information systems security research literature has witnessed limited efforts at theoretical development (Dhillon and Torkzadeh, 2006). There are few research studies involving adequate empirical findings from a substantial research process with appropriate theoretical underpinnings. In this chapter, we developed a critical synthesis of the current philosophical debate about information systems security. Such an exercise informs us about the potential and the impact of various approaches. It informs us about the limitations of different approaches as well. To trace the complexity of information systems security we have defined the set of beliefs and assumptions about the nature of

social reality. The analysis of the philosophical debate has implications for possible theoretical improvements. The literature review combined with the above discussion suggests that the contextualist perspective is the way forward for the maturing of the information systems security discipline.

2.5 Conclusion

The contribution of the chapter is as follows. First, it presents the philosophical foundations of socio-organizational information systems security research. The literature review identifies the prominence of formistic and mechanistic perspectives, which may be attributed to the belief in analytic theories during the early stages of a discipline. The critique of current approaches lays the foundation for a contextualist perspective in dealing with security issues. This standpoint is also aligned with the need for research that employs a synthetic theoretical position for the security discipline to mature. Finally, there is potential for empirical studies grounded in a contextualist perspective to help improve the security posture of an organization.

CHAPTER 3

Research Methodology

3.1 Introduction

The purpose of this chapter is to establish the research methodology for investigating strategic information systems security initiatives. It is important to understand the philosophical considerations of the research approach adopted. The underlying philosophical assumptions would guide the research methodology. At the same time, it is imperative for the researcher to acknowledge the role of theory in a research study.

This chapter is organized into five sections. Following a brief introduction, section 3.2 outlines the philosophical assumptions underlying this research. Section 3.3 provides the theoretical perspective adopted to conduct the research. The argument and research questions are also explicated in this section. Section 3.4 presents the research design. The chapter concludes with section 3.5.

3.2 Philosophical Considerations

In the philosophy of science, ontology and epistemology are two of the most central concepts. Ontology refers to the nature of reality. It points to the claims or

assumptions that a particular approach to social inquiry makes about the nature of social reality (Blaikie, 1993). According to Burrell and Morgan (1979), ontological assumptions are concerned with whether the reality to be investigated is externally imposed on the individual mind or is produced internally to an individual and is a product of their cognition. In general, there are two positions on ontological assumptions pertaining to social enquiry: realist and constructivist. The realist position assumes that there is a single social reality which is ordered in nature. The constructivist position assumes that there are multiple social realities which are pre-interpreted and inter-subjective in nature.

Epistemology addresses how to gain knowledge of the social reality. According to Blaikie (1993), an epistemology is a theory of knowledge; it presents a view and a justification for what can be regarded as knowledge. According to Burrell and Morgan (1979), epistemological assumptions are about the nature of knowledge and how one might understand the world and communicate it to others. In general, there are two basic positions on epistemological assumptions pertaining to social enquiry. These are outside and inside positions (etic versus emic). The outside (etic) position entails social reality as existing independently of the observer. The social reality can be directly observed and explained. The inside (emic) position considers social reality to be produced and reproduced by actors. This suggests that the social world can only be known by understanding the local language, meanings, culture and social rules associated with the actors involved in the activity of interest. In other words, the social world can be properly grasped by adopting the social actor's point of view.

At an epistemological level, positive and interpretive approaches to social enquiry are associated with outside and inside positions respectively. Burrell and Morgan (1979) name the outside and inside positions of epistemological debate as positivism and anti-positivism respectively. Myers (1997) considers three categories of approaches to social enquiry: positivism, interpretivism and critical theory. Guba (1990) and Schwandt (1990) follow a similar classification although they term interpretivism as constructivism. For Blaikie (1993), the outside epistemological position involves positivism, critical rationalism and realism as the major approaches. Interpretivism, critical theory, structuration theory and feminism are the prominent approaches for the inside epistemological position (Blaikie, 1993).

In this research, the epistemological assumptions adopted are from the interpretive paradigm. The purpose of interpretive research is to understand the meaning of social action. According to Blaikie (1993), interpretivism entails an ontology in which social reality is regarded as the product of processes by which social actors negotiate the meanings for actions and situations. It is a complex of socially constructed meanings. In terms of epistemology, interpretivism entails derivation of knowledge from everyday concepts and meanings.

The social researcher enters the everyday social world in order to grasp the socially constructed meanings, and then reconstructs these meanings in social scientific language (Blaikie, 1993: 96).

A researcher herself is an instrument of observation (Lee, 1999). The researcher enters the everyday world of social actors. She presents the account of these actors as her interpretation or understanding of the meanings of these social actors' actions. The

social world, for interpretivism, is the world perceived and experienced by its members; and their behavior depends on how they (as individuals) interpret the conditions in which they find themselves. As such, we could say that social reality is already interpreted or is preinterpreted. According to Blaikie (1993), the reconstruction of meanings can be regarded as social scientific descriptions from which social theories or perspectives could be developed. These theories or perspectives shape decision-making, which in turn shapes the reality.

The socially constructed reality has both objective and subjective dimensions. The objective dimension is observable human behavior. According to Lee (1991), the social scientist must take into consideration and account for (in terms of collecting facts and data) both purely objective and the subjective meaning that the behavior has for the human subjects themselves. Lee (1999) also states that the validity of an interpretation can be assessed. This characteristic is based on the argument that people know what they are doing. As such, one should be able to understand the rationale behind an action. This in turn leads to the assessment of the goodness of the interpretation.

3.3 Theoretical Considerations

To conduct the research study theoretical considerations must be established. In conducting organizational research, Eisenhardt (1989) believes the role of theory contributes at three levels. That is, theory can be used as an initial guide to design and collect data, as an iterative process to collect and analyze data, or as a final product of the research. Yin (1989) points that the role of theory prior to data collection is often

overlooked in case study research. In elaborating upon the use of theory, Walsham (1995) emphasizes the importance of creating an initial theoretical framework that takes account of previous knowledge and forms a sensible theoretical basis for the empirical work. In fact, Denzin and Lincoln (2000) believe a researcher should approach the world with an apriori framework or theory. At the same time, there is a potential problem “of the researcher only seeing what the theory suggests” (Walsham, 1995). In other words, prior theory held by a researcher can influence what is to be observed (Smith and Deemer, 2000). The research on information systems should be informed by general theories on the nature of organizations (Walsham 1995).

The theoretical considerations are discussed next. This section outlines the argument of the research and provides research questions guiding this research. The section on theoretical perspective explains the theory used to conduct this research.

3.3.1 Research argument and questions

The argument of this dissertation is that in order for strategic information systems security initiatives to be successful a proper undertaking of the content, context and process of formulation and implementation of a security initiative is essential. The business world is comprised of events with disorder and change as its key features. To attain success with a security program, the dynamics of security change under different contexts need to be accounted for and properly understood. The contextual analysis of a security initiative involves investigation at the vertical level, the horizontal level and the interconnections between them. The vertical level involves context at various levels

including both outer and inner environment in which an organization operates. The horizontal level captures the historical, present and future time of a continuing system, a corporate entity. As such, an appropriate security change effort needs to be grounded in contextualism to be instituted in an organization.

Accordingly, this dissertation addresses the general research question about how to institute strategic information systems security change initiatives in an organization.

The further sub research questions are:

- What aspects of information systems goals, policies and programs should be included in a strategic information systems security initiative?
- How should strategic information systems security initiatives be formulated and implemented in an organization?
- Why and in what manner does the inner and outer environment of an organization impact the strategic information systems security initiatives?

3.3.2 Theoretical perspective

In this research, the business world is considered to be uncertain, and complex. This provides the basis to view change as an iterative and multilevel process. Pettigrew (1990) contends that change forces the players to deal with continuity and change, actions and structure, endogenous and exogenous factors, as well as the role of chance and surprise. The change is comprised of political, cultural, incremental, environmental, structural and rational dimensions (Pettigrew, 1990).

The present study adopts a contextualist theory of strategic change developed by Pettigrew (1987) as the theoretical basis. To study transformations in firms, it is essential to adopt a holistic and dynamic analysis of change rooted in historical, processual and contextual aspects is essential (Pettigrew, 1990). The historical aspects imply the evolution of ideas and actions for change, while the processual aspects emphasize action and structure overtime. The contextual aspects represent the relationship between process and contexts.

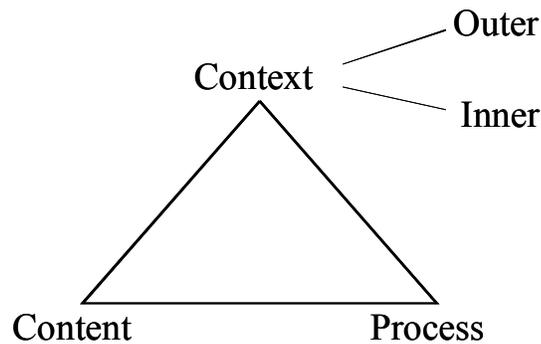
The underlying assumption of contextualist theory is that organizations are political and cultural systems. An organization can be explored as a continuing system where legitimacy serves as the link between political and cultural analyses. It is imperative to understand the processes and mechanisms used to legitimize and delegitimize strategic changes (Pettigrew, 1987). “The content of strategic change is thus ultimately a product of a legitimation process shaped by political/cultural considerations, though often expressed in rational/analytic terms” (Pettigrew, 1990). In other words, “the context of strategy can be mobilized to legitimate the content and the process of a strategic adjustment” (Pettigrew, 1985).

The contextualist theory of strategic change posits that transformation of the firm can be understood by exploring the content, context, and the process of change together with their inter-connections through time (Pettigrew 1987). The formulation of the content of any strategy needs to acknowledge the management of its context and process. The three central components of this theory are summarized below:

Content. The content as analytic category refers to the particular areas of transformation under examination (Pettigrew, 1987). It addresses the ‘what’ of change. Content is composed of assumptions, objectives and strategic choices of the firm.

Process. The process category addresses the ‘how’ of change. It refers to the actions, reactions and interactions of stakeholders in the transformation of the firm. According to Pettigrew (1985), the process is regarded as “a continuous, interdependent, sequence of actions and events which is being used to explain the origins, continuance and outcome of some phenomena.” It involves the formulation and implementation of strategy.

Context. The context category involves the inner and outer context of the firm (figure 3.1). Outer context involves the external social, economic, and political environment in which the firm operates. Inner context is the internal structural, cultural and political environment of the firm. It addresses the ‘why’ of change. “Context is not just a stimulus environment but a nested arrangement of structures and processes where the subjective interpretations of actors perceiving, comprehending, learning and remembering help shape process” (Pettigrew, 1990).



**Figure 3.1: Contextualist model of strategic change
(reproduced from Pettigrew, 1990)**

3.3.3. Theoretical framework to conduct argument

This research adapts the contextualist theory of strategic change as the theoretical framework to understand the strategic information systems security initiatives undertaken in an organization. The analytical categories of this theory are used to identify the critical dimensions of interest for investigating security initiatives. These dimensions form the conceptual basis for the research study.

There are three analytic categories (table 3.1) in the contextualist theory of strategic change that guide our understanding of strategic security initiatives. In the initial step, the content of a strategic security initiative is identified. The security policy of an organization is analyzed. This should be in alignment with the overall security goals and objectives of that organization. Further, the extant security guidelines and procedures are also analyzed. In the next stage, the concern is to understand the context in which the firm operates. The context is analyzed in terms of information systems security aspects. The scrutiny of inner context leads us to study the prevalent security

culture. The security culture also impacts the governance structures in place, which is analyzed along with the associated political system. An understanding of outer context, which includes socio-economic and competitive environment, is also essential. Here, the government regulations and laws to establish a standard level of practice are further reviewed. For the analytic category of process, the formulation and implementation of strategic security initiatives is examined.

Table 3.1: Analytic categories of contextualist security change

Analytic categories	Description	Factors of interest in information system security
Content	Particular areas of transformation under examination	Security goals and objectives, security policy, security standard, security program
Inner context	Intra-organizational environment of the firm	Security culture, security governance structure
Outer context	External environment in which the firm operates	Regulations, laws, competitive environment
Process	Continuous, interdependent, sequence of actions and events	Formulation and implementation of strategic security initiatives

The aim of the theoretical framework is to guide a researcher during empirical work. It is not meant to provide a rigid structure. A degree of openness to the field data is required in interpretive field research (Walsham, 1995). The researcher should be willing to modify initial assumptions and theories if new developments in the research study become apparent.

3.4 Research Design

The research design for contextualist interpretation of strategic information systems security initiatives is discussed under research strategy, unit of analysis, data collection and data analysis.

3.4.1 Research strategy

This research follows an in-depth case study method using a qualitative approach in the interpretive tradition. A case study is an empirical inquiry that investigates a contemporary phenomenon within its real-life context, especially when the boundaries between phenomenon and context are not clearly evident (Yin, 1989). It refers to the examination of a real-world event as it actually exists in its natural, real-world setting (Lee, 1989). The case study method is appropriate for research problems in their formative stages, where the experiences of the actors and the context of action are critical (Benbasat et al., 1987). Using a case study allows the researcher to ask penetrating questions and capture the richness of organizational behavior (Gable, 1994). Walsham (1995) contends that four types of generalizations can be developed from an interpretive case study research. These are development of concepts, generation of theory, drawing of specific implications, and contributions of rich insight.

The appropriateness of the case research strategy can be judged by employing the criteria as outlined by Benbasat et al. (1987). In this research, the phenomenon of interest needs to be studied in its natural setting. Secondly, the focus of the research study needs to be on contemporary events. Thirdly, the research process does not

require control or manipulation of subjects and events. Finally, although the research problem is investigated using an established theoretical case such an inquiry mainly provides insight into an issue. Case studies provide a supportive role to facilitate deeper understanding of the issue, which then advances knowledge. This is the feature of an instrumental case study. In this type of case study, “the case still is looked at in depth, its contexts scrutinized, its ordinary activities detailed, but all because this helps the researcher to pursue the external interest” (Stake, 2000).

Many researchers (for instance, Guba and Lincoln, 1989; Marshall, 1990; Golden-Biddle and Locke, 1993; Walsham, 1995; Walsham and Sahay, 1999; Klein and Myers, 1999; Madison, 1988; Trauth and Jessup, 2000) provide the criteria to check the validity of a case study in the interpretive tradition. This dissertation uses the evaluative criteria guidelines proposed by Klein and Myers (1999). These criteria are summarized in table 3.2.

3.4.2 Unit of analysis

Multiple-case designs are desirable when the intent of the research is description, theory building, or theory testing (Yin, 1989). Such a design allows for cross-case analysis. Further, multiple cases yield more general research results (Benbasat, 1987). In the present research process, two government organizations were identified based on the selection criteria to conduct the research. These two organizations are Information Technology Agency (ITA) and Department of Transportation (DOT). The two sites satisfy the site selection criteria as advocated by

Yin (1989). This criteria entails selection of sites where similar results may be used as "literal" replications, and where contradictory results may be chosen for "theoretical" replication. With careful site selection, the researcher can extend and revise the initial propositions of the study.

**Table 3.2: Evaluative criteria for interpretive case study
(adapted from Klein and Myers, 1999)**

Klein and Myers (1999) criteria	Explanation
The Hermeneutic Circle	All human understanding is achieved by iterating between considering the interdependent meaning of parts and the whole that they form. This principle of human understanding is fundamental to all the other principles.
Contextualization	Requires critical reflection of the social and historical background of the research setting, so that the intended audience can see how the current situation under investigation emerged.
Interaction Between the Researchers and the Subjects	Requires critical reflection on how the research materials (or "data") were socially constructed through the interaction between the researchers and participants.
Abstraction and Generalization	Requires relating the idiographic details revealed by the data interpretation through the application of principles one and two to theoretical, general concepts that describe the nature of human understanding and social action.
Dialogical Reasoning	Requires sensitivity to possible contradictions between the theoretical: preconceptions guiding the research design and actual findings ("the story which the data tell") with subsequent cycles of revision.
Multiple Interpretations	Requires sensitivity to possible differences in interpretations among the participants as are typically expressed in multiple narratives or stories of the same sequence of events under study. Similar to multiple witness accounts even if all tell it as they saw it.
Suspicion	Requires sensitivity to possible "biases" and systematic "distortions" in the narratives collected from the participants.

Information Technology Agency (ITA) is a state technology agency operating in the southeastern part of the US. At the time of this study, the organization was engaged in the development of an information systems security program with a strategic focus.

The organization and the security program are unique. ITA is a consolidated and centralized state government agency for the IT needs of all government agencies in the state. It is responsible for the operation of IT infrastructure, governance of IT investments, and procurement of technology in the state. The information systems security efforts at ITA are an interesting effort to develop an integrated security program in a federated environment. This case was selected because the organization was in the process of formulating security initiatives for the entire state to protect IT assets of all state agencies.

Department of Transportation (DOT) is a state transportation agency that is also located in the southeastern part of the US. At the time of study, the organization was engaged in implementing a strategic information systems security program that had been developed by the state. DOT is responsible for building, maintaining and operating the state's roads, bridges and tunnels. It also provides funding for airports, seaports, rail and public transportation. DOT has been mandated by state legislation to comply with the state information security policy and standards. As such, the organization had to reconfigure its existing security approach to meet the requirements of new state security initiatives. This case was chosen because the organization was in the process of implementing security initiatives in a federated environment. Another interesting feature was that the organization's IT operations were outsourced to another state agency. This essentially meant that DOT had to rely upon an outsourcing firm to ensure adequate technical security controls and measures, although DOT was responsible for protection against adverse security events.

The primary reason to select the two organizations is because these provided an opportunity to learn (Stake, 2000). Both organizations were involved in developing and implementing different facets of information system security initiatives with particular attention to future needs in the changing business environment.

3.4.3 Data collection

The techniques that do not jeopardize the ability to observe in-the-moment reactions and behaviors were used for data collection in this research study. Also, the data collection techniques need to abstain from being intrusive. As such, semi-structured interviews and informal conversations with participants served as the primary method for data collection. The interviews were conducted at different management levels. A list of organizational members interviewed at ITA and DOT appears in appendices A and B. The stakeholders were identified and interviewed from within the security departments, as well as, other departments across the two organizations. In all, thirty-three organizational members were interviewed from the ITA and twenty-nine members were interviewed from the DOT. Participation in the interviews was voluntary and informed consent of the participants was obtained prior to the interviews.

Interviews were conducted based upon a topic guide developed from the theoretical framework. Topic guides were customized for each interview. Hand-written notes were taken during the interviews. These were updated and transcribed immediately after the interview to ensure all details were captured. None of the interviews were tape-recorded, which helped to build a level of trust with participants

and allowed the researcher to repeatedly observe events in contextualized detail. This was considered to be more important and enriching than to capture exact words spoken just once. Additional sources of data included participant written-cases, group sessions, community meetings, documentary and archive data. The field notes were recorded into a notebook computer. Qualitative data analysis software, Atlas Ti, was employed to develop conceptual maps for the problem situation at Department of Transportation. In general, findings emerging from data collection and analysis were shared with an informant in each organization for validation purposes.

3.4.4 Data analysis

The empirical evidence collected in the form of data from interviews and secondary sources indicated a variety of different issues. These were evaluated with respect to the research framework. The triangulation of data was achieved by verifying the empirical evidence with an informant in each respective setting. The research findings were interpreted consistently with the ontological beliefs of this research. By abiding with the tenets of interpretive research, the resulting principles of this research are expected to be useful in settings other than the government sector.

3.5 Conclusion

This chapter outlines the research methodology adopted in this study. The methodology is based on ontological and epistemological considerations. An interpretive

approach of inquiry is used to conduct this research. This approach is justified based on the nature of the research problem and the theoretical perspective adopted.

CHAPTER 4

A Contextualist Interpretation of Strategic Information Systems Security in Organizations

4.1 Introduction

This chapter provides a description of the organizations used in this dissertation research work. The organizations are studied utilizing the contextualist theoretical framework as presented in chapter 3. As per the research framework, an organization should be analyzed in terms of its context, content and processes. The next section provides a description of the Information Technology Agency. The organizational context, content of the program and associated processes are described under this section. The subsequent section analyzes the Department of Transportation using a similar structure. The chapter ends with a brief discussion of issues that emerged based on the theory of contextualist strategic change.

4.2 Information Technology Agency

The Information Technology Agency (ITA) is a state technology agency that is located in the southeastern part of the US. It is a consolidated and centralized government agency for the state of Wonderland. ITA is responsible for providing

information technology (IT) services to about ninety government agencies within the state. In essence, it is a behind-the-scenes service provider. ITA is responsible for the operation of the IT infrastructure, governance of IT investments, and procurement of technology in Wonderland. The emphasis of the agency has been to create accountability for public funds being spent on technology in the state. The goal is to become a leader in the use of technology in government across the country. This is to be achieved by transforming the IT environment, keeping costs consistent with market, and achieving results by reinvesting savings. In 2007, the agency had an operating budget of about three hundred million dollars.

Information systems security initiatives in the state of Wonderland are primarily the result of efforts by the governor's office. In the wake of a financial crisis in 2001, the Governor decided to centralize IT efforts for the entire state. At that time, various government agencies were developing IT systems and programs spending thousands of tax dollars. The governor believed that significant financial gains could be achieved if such duplication of systems or efforts was reduced across the state. As such, centralization of technology efforts seemed to be a viable solution to mitigate the financial budget problems. Budgetary restraint was a key driver behind IT consolidation efforts in Wonderland.

During the same period, there was public concern for the government to protect the public's information privacy rights. There had been an increased number of incidents involving loss of personal and financial information of citizens at several government agencies. Such incidents threatened potential losses that might damage the

lives and finances of individuals. There were also concerns from the federal government to protect personal information pertaining to citizens. In recent years, the federal government has enacted regulations and acts, such as Sarbanes-Oxley Act, Health Information Privacy Protection Act, for various industries to force the organizations to protect the information resources of citizens. In short, there was growing concern for privacy at the national level. The context, content and process of information system security initiatives at ITA are described in the rest of this section.

4.2.1 Context

The Governor of Wonderland pushed for information technology reforms in the state in order to address the growing budgetary concerns, privacy concerns, and also the promise of delivering efficient management to the state. These reforms were well received by state legislators who unanimously approved them. The reforms led to the creation of several new functions and positions for the state: Secretary of Technology, Technology Investment Board (TIB) and Chief Information Officer (CIO). The new legislation mandated the Secretary of Technology to achieve IT consolidation and secure the IT environment for the state. The reforms led to the creation of ITA in 2003 and consolidation of IT infrastructure and related resources from other state government agencies. ITA was to provide all IT related services to the agencies. However, agencies were allowed to have in-house IT application development teams. The personnel for different positions at ITA were selected from the entire employee pool of state

government agencies that had IT expertise. As can be expected, the formation and existence of ITA was complex.

The early days of ITA were marred with problems and issues related to operational procedures. Much confusion surrounded daily operations due to the scope of the agency. Such a scope could be challenging for any organization especially the one without any prior expertise in handling services on such a large scale. Despite these concerns, the state was lauded for its efforts and won several national awards. However, the failings were real and there was growing anxiety over how to handle the IT situation of the state. Given these concerns, the change in government called for a new direction in technology efforts.

Regulatory environment

In 2002, Wonderland passed a bill that authorized the Secretary of Technology to conduct technology security audits for the state agencies. In response, the Strategic Plan for Technology for 2002-2006 from the Secretary of Technology Office stipulated that the CIO of ITA should develop and implement an IT security program for the entire state. In addition, the CIO had the responsibility to create a statewide information security office, and to develop evaluation tools to measure the cost savings generated by a statewide security program.

By 2003, legislation was passed to create ITA and the CIO was appointed around January 2004 by the Technology Investment Board (TIB), which oversees ITA. The legislation mandates that the TIB and the CIO establish security policies,

procedures and standards for the executive branch agencies of the state. The legislation also details directions to the CIO pertaining to security of government database. Per this legislation,

The CIO shall direct the development of policies, procedures and standards for assessing security risks, determining the appropriate security measures and performing security audits of government databases and data communications. At a minimum, these policies, procedures and standards shall address the scope of security audits and which public bodies are authorized to conduct security audits.

The CIO charged the Chief Information Security Officer (CISO) with development of information security policies, procedures and standards to protect the confidentiality, integrity, and availability of the state's information assets. In accordance with the legislation, all government agencies are responsible for complying with the state security policies and standards. In addition, the legislation requires each agency to report to ITA all security incidents that have the potential to compromise security of the IT infrastructure. Such incidents must be reported within twenty-four hours of occurrence.

An important factor influencing the security program at ITA was the state security audit report. In 2006, the General Assembly of the state passed a resolution directing state auditors to report on the adequacy of security of state government databases and data communications. As a result, the ITA was required to develop an action plan to respond to this audit report. The current state of security program developed by ITA is in direct response to the recommendations provided by the audit report. In 2007, the Governor issued an executive order that empowered the Secretary

of Technology to ensure compliance with the state's information security policies and standards.

Competitive environment

The ITA operates in a federated environment supporting the digital needs of government agencies in the state. The primary motive of a government organization is to provide efficient service to citizens. Prior to the formation of the ITA, each state agency was responsible for its own IT infrastructure and associated technical services. Not surprisingly, there was enormous duplication of efforts in terms of technology development resulting in waste of critical resources. To reduce this waste of tax dollars, the state government consolidated the IT infrastructure of the entire state to ITA, as well as the responsibility of IT related support for the executive branch agencies. In addition, ITA became accountable for the governance of IT investments in support of the duties of the TIB and the CIO of the state. Finally, ITA was made responsible for procurement of technology for the entire state. In essence, IT infrastructure and services moved from individual agencies to ITA. Thus, all network support staff became employees of ITA as well. This implied that employees were reporting to supervisors who did not work for and were not affiliated with or familiar with the services of the agencies that their staff supported.

The financial considerations for the ITA are rather interesting. The state legislators directed the ITA to fund operational expenses through direct charges to agencies. That is, ITA is following a fee-for-service model. The practical impact of this

decision was that certain expenditures to meet legislative mandates and minimum standards would be reflected in additional charges to affected customer agencies. In addition, agencies have to pay the ITA for services rendered. As a result, the ITA started to charge the agencies a five-and-a-half percent fee for each employee that provided services to that agency. So, not only did agencies still pay the employees salary, they now paid an additional five-and-a-half percent of that salary directly to the ITA. On recommendation by the TIB, the Governor approved an agreement with the Outsourcing Firm in 2005 to modernize the state's IT infrastructure. The ten-year partnership valued at around two billion dollars is expected to result in about three hundred million dollars capital investment in the state.

In 2006, the Outsourcing Firm took responsibility for the operations and management of all IT infrastructure components, such as desktops, servers, mainframes, and routers for agencies that the ITA serves. However, the TIB, the CIO and the ITA itself continued to retain responsibility for the state's IT security governance. As per the contract, the ITA specified the required information systems security standards and controls for the state agencies. The Outsourcing Firm was to use that information to ensure their operations meet the state's security standards. As such, the ITA took on the role of a middleman between the state agencies and the Outsourcing Firm. As part of the partnership, the Outsourcing Firm accommodated around five hundred and fifty ITA employees who accepted enhanced job offers in the first phase of the job-offer period. Political pressure forced legislators to give employees an option to move to the Outsourcing Firm. This was done to minimize the impact to employees as a result of the

Outsourcing Firm partnership. In essence, many employees saw their job functions being outsourced from the ITA and then to the Outsourcing Firm. The partnership with the Outsourcing Firm has added increasing complexity to the already complex operational environment in Wonderland.

In the case of information systems security, all agencies have to be compliant with the state security policy and standard. Now, agencies face a dilemma. It makes sense to have their security measures evaluated by the ITA, as they are the developers of the security policy and standard. An audit so conducted by the ITA would point to gaps in security. In order to plug these gaps, the agency would have to rely on the ITA to provide appropriate service and would have to pay for these services as well as the evaluation. The problem is that the state agencies were concerned that the ITA would inflate their services to coincide with their monetary requirements. Agencies do not necessarily have to purchase the services of the ITA. However, there is only one government agency that provides IT security services in the state. As such, agencies have to turn to the ITA for support. Although it seems that leverage has been provided to agencies to make their decisions, they are restricted to the ITA and the Outsourcing Firm for their IT needs. Thus, state agencies are being forced by politics and law to deal with the ITA.

Organizational Structure

The CIO is at the helm of organizational structure at the ITA. This position must be approved by the state assembly and is appointed for a period of five years. The CIO

essentially serves as ITA's chief administrative officer and leads the organization to attain IT governance and operational excellence in the state. The CIO is appointed by the TIB, which serves in a capacity similar to a board of directors in private organizations. The TIB acts as an oversight committee that reviews technology investments across state government agencies and the board members are appointed by the Governor, the General Assembly and the Secretary of Technology. The aim of the state government is to select members from industry who would bring substantial experience from the business world and contribute to IT reforms in the state.

The ITA is divided into eleven internal directorates. However, the organization is viewed in terms of six functional areas for reporting and planning purposes (figure 4.1). The Customer Management directorate is responsible for maintaining business relationships with customers, which include government agencies in the state. The purpose of the directorate is to help agencies identify technology requirements and integrate IT with business strategies. The IT Solutions directorate has three areas of responsibility and provides statewide IT governance and oversight services. In this capacity, the directorate helps in formulating strategy for future IT direction in the state. Also, it provides guidance in implementing specific technology initiatives. In addition, the directorate extends its technical expertise to develop statewide technology solutions. Finally, it is responsible for the development and support of technology applications for internal use at ITA.

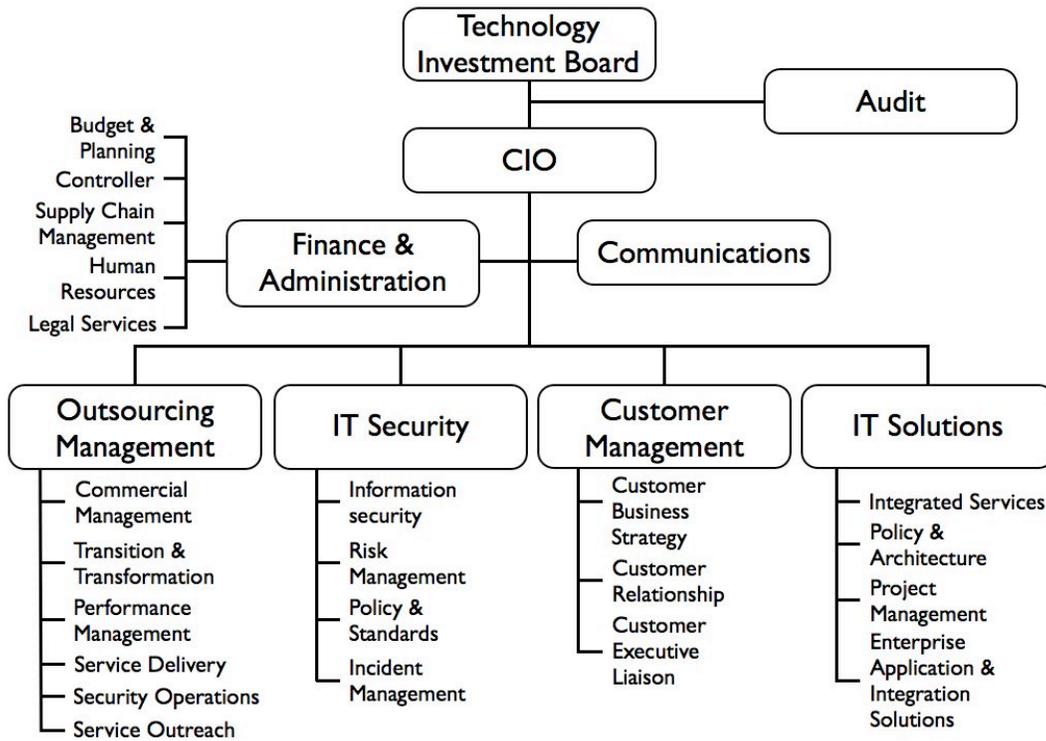


Figure 4.1: Organizational structure of the Information Technology Agency

The aim of the Audit directorate is to provide objective assurance and consulting services. The directorate is responsible for evaluating the effectiveness of risk management, control and governance processes. The Finance & Administration directorate is concerned with financial and procurement responsibilities. It performs the functions of supply chain management, financial management, internal performance measurement, and human resource management. The Outsourcing Management directorate is focused on managing the IT infrastructure partnership between the ITA and the Outsourcing Firm. The directorate must interact daily with the Outsourcing Firm for technical operations, service delivery, and also ensure that proposed

technology solutions are appropriate from a security standpoint. It also provides an operational and tactical interface to customer agencies. Finally, the directorate is responsible for contractual aspects, and also provides oversight and assurance of partnership operations.

The IT Security directorate provides information technology security support to the state. It is responsible for security assurance activities and ensures a secure IT environment for agencies. It also provides a framework for IT security program based upon principles of confidentiality, integrity and availability. The director of the IT Security directorate also serves as the CISO of the state. In this capacity, the CISO is required to protect state information while providing information security governance services. For the ITA, the CISO is expected to provide information security risk management services. The director is assisted by the Deputy CISO to protect the state information through IT security. The Deputy CISO is responsible for managing daily operations for the directorate. She is also expected to coordinate the state Information Security Officer (ISO) program. As per initial structure of the ITA, the Security Advisory Group (SAG) supports the CISO in an advisory role. However, the SAG is now a forum to enhance communication between the security department at the ITA and other agencies. The SAG is comprised of ISOs from different agencies of the state and meets on a monthly basis.

The security directorate is internally organized into six functions (figure 4.2). One of the main functions of the directorate is to define IT security program for the state. The directorate must develop IT security policies, standards and guidelines for

statewide implementation. A manager has been assigned the task to develop and revise policies, including configuration and policy standards and exemptions of customer agencies. Another vital function is information security assurance which assesses the security posture of the state. An assurance manager is responsible for performing this function by employing security audit reports and security assessments of high-risk systems. The responsibility also involves managing the Security Services Information Security Data Warehouse, which provides a central repository listing of all the state's sensitive systems and relative security controls. The manager is assisted by two security analysts to analyze IT security requirements and controls, and vulnerability assessments.

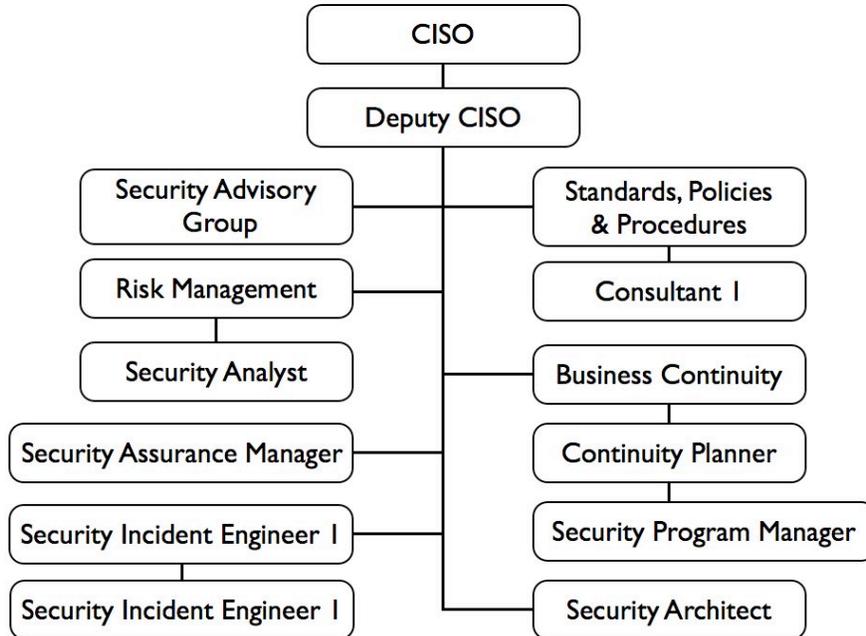


Figure 4.2: IT security directorate of the Information Technology Agency

The Information Security Architecture function is responsible for developing a standard IT security architecture for the state. A security architect is expected to assess IT systems and network designs to enable a secure technology structure. In case of an incident, the incident management function at the directorate is expected to serve as the IT Security Incident Response Team. The Director of this function would provide analysis and response to the security incident as a technical expert. An engineer is responsible for daily activities that include collection, analysis, and classification of security incidents.

The Critical Infrastructure Protection & Service Continuity function is concerned with physical security, personnel security and developing continuity of operations plan (COOP). The function manager is expected to provide oversight for the records management of the security directorate, the security awareness program, and physical security of ITA facilities. The security awareness and training function uses different approaches including face-to-face and online awareness training for organizational members. The function manager is also required to coordinate disaster recovery planning with agencies. She is assisted by a planner for business continuity planning, while the security program manager provides support for physical and personnel security.

The organizational structure is dynamic to meet emerging needs of the environment. For instance, the position of Information Assurance manager was created although such a position was not outlined in the original structure. As the organization matured, the security department was restructured to assume a governance role. The

CISO position was subsequently changed to Chief Information Security & Internal Audit Officer (CISIAO). In essence, the IT Security and Audit directorates were merged under single leadership. Further, the development of a Security Council is another indicator of the flexibility of the management team. This council was developed as the nature of SAG emerged to be different than its intended advisory role. The aim of the Security Council is to provide advice to the security department on how to improve security services for state agencies. The emphasis of the directorate has been to develop well-articulated roles and clearly defined organizational structure.

4.2.2 Content

The contextualist theory of strategic change posits that transformation of the firm can be understood by exploring the content, context and the process of change together with their interconnections through time (Pettigrew, 1987). The formulation of the content of any strategy needs to acknowledge the management of its context and process. The content as analytic category refers to the particular areas of transformation under examination. It addresses the ‘what’ of change. Content is composed of assumptions, objectives and strategic choices of the firm. In the initial step, the content of strategic information systems security initiatives is identified, followed by a description of security policy. The security policy should be in alignment with the overall security goals and objectives of that organization. The information systems security standard and guidelines supporting the ITA security policy are described in this section.

Information systems security objectives

ITA is focused on protecting data, software, hardware, and communications of the state. The security program is intended to protect IT systems and data from credible threats, whether internal or external, deliberate or accidental. The overall objective of the security program is to protect the state's data against unauthorized access and use; to maintain the integrity of data; to meet requirements for data residing on IT systems; and, to meet federal, state and other regulatory and legislative requirements. The ITA adopted the traditional view of information security and based its program on the principles of confidentiality, integrity and availability of data. The principle of confidentiality ensures that information is shared among authorized persons or organizations only. Integrity is concerned with the correctness of the information as well as whether it can be trusted and relied upon. Availability implies that the systems required for delivering, storing and processing information are accessible when needed and by those who need them.

Information systems security policy

The ITA has an elaborate IT security policy which became effective in July 2006. This policy superseded the earlier IT security policy dated 2001. The aim of the policy is to protect the state IT systems and data from various threats. The focus is on confidentiality, integrity, and availability principles of information systems security. This policy clearly defines various security roles and responsibilities in the

organization. It also explicates the IT security program as well as the requirements for compliance. Finally, it details the necessity for IT security audits and protection of IT resources. The formally stated purpose of the policy is to protect state information technology assets and information processed by defining the minimum information technology security requirements for state agencies.

The policy details responsibilities of the ITA, as well as, differentiates between those of an agency. In general, the ITA is charged with developing security policy and programs while the agencies are charged with adequately implementing the policy. This again reflects the nature of the relationship that exists between the ITA and different agencies, which are its customers. The twenty-three pages policy document has come a long way from its predecessor one page security policy of 2001. The old IT security policy (2001 version) recognized the reliance of various agencies on information systems. It is quite interesting to see the use of the term ‘information systems’ in the old document compared to the shift in current 2006 policy to IT systems. Further, the policy also recognized differences in the information environment of various agencies and left it upon the agencies to develop an appropriate structure of IT security.

The new security policy clearly defines the role of the CIO, the CISO and other security officers for the ITA. The policy addresses the responsibilities of the Agency Head and various IT users as well. The roles addressed include the ISO, the privacy officer, the system owner, the data owner, the system administration, the data custodian and the IT system users. The policy briefly describes the security program to be in place in order to protect state IT systems and data. The program involves nine functional

components which target protection of various systems and data based on sensitivity levels. Each of these components has a supporting guideline, which provides detailed procedures on how to implement the specific component. These components as presented in the state security policy are briefly discussed in the remaining part of the section.

The first step in *risk management* is to conduct a business impact analysis (BIA). This analysis identifies those business functions that are essential and are dependent on IT. After completing BIA, agencies are to classify the sensitivity of IT systems and data. Then, agencies have to determine ownership of all sensitive IT systems so that IT security roles can be appropriately assigned. A periodic, formal risk analysis is required for all IT systems classified as sensitive. The risk analysis process assesses threats to IT systems and data, probabilities of occurrence and the appropriate security controls necessary to reduce these risks to an acceptable level. The sensitive IT systems require periodic, independent *security audits*. These audits are necessary to determine whether the overall protection of IT systems and data they handle is adequate.

The purpose of *IT systems security* is to define steps necessary to provide adequate and effective protection for agency IT systems in the areas of IT systems hardening, systems interoperability security and systems development life cycle security. Another component addressed in the policy is *logical access control (LAC)*. This component defines steps necessary to protect the confidentiality, integrity, and availability of IT systems and data against compromise. The LAC requirements identify the measures needed to verify that all IT systems users are who they say they are and

that they are permitted to use the systems and data they are attempting to access. This component defines requirements in the areas of account management, password management, and remote access. The *data protection* provides security safeguards for processing and storing of data. This component of the security program outlines methods to safeguard data in a manner commensurate with the sensitivity and risk involved.

The *IT contingency planning* defines processes and procedures necessary for recovery and restoration of IT systems and data in case of an event that renders these unavailable. It includes continuity of operations planning and disaster recovery planning. The *facilities security* safeguards provide a first line of defense for IT systems against damage, theft, unauthorized disclosure of data, loss of control over system integrity, and interruption to computer services. The component of *personnel security* outlines access determination and control requirements that restrict access of IT systems to those individuals who require such access as part of their job duties. This component also includes security awareness and training requirements regarding security policy.

The *threat management* addresses protection of IT systems and data by preparing for and responding to IT security incidents. This component of the security program includes threat detection, incident handling, and IT security monitoring and logging. The *IT asset management* concerns protection of the components that comprise IT systems by managing them in a planned, organized, and secure fashion. It includes asset control, software license management, and configuration management. In terms of compliance with IT security policy and standards, the policy emphasizes monitoring,

audits, and confiscation and removal of IT resources. For monitoring, the policy states various monitoring activities and no expectation of privacy for the users. It also provides information on what is to be monitored and authorization for such.

The state legislation ascribes the CIO of ITA with the responsibility of performing *security audits* of government databases and data communications. Such audits are to be conducted annually and require compliance with ITA's security policy and standard. The audits can be conducted by CISO personnel, agency internal auditors, the state public auditors, or staff of an appropriate private firm. The audit report must be submitted to the respective Agency Head, who will develop a required action plan based on the report. Finally, the policy describes a provision for Agency Heads to request any exceptions from the IT security policy. Such requests must clearly identify any reasons for the exception and identify the appropriate controls that are in place.

The current state security policy appears to be simply a current version of the older 2001 version of the security standard. The old standard was comprised of thirteen components which formed the security program. These components were reorganized into a smaller set of components in the new policy document. The older security policy was very broad in nature and did not reflect an appropriate level of granularity. The new security policy advocates a security program which has nine components that seem to have evolved from the earlier thirteen components.

Information systems security standard

The security standard for the ITA became effective on July 2006. The standard was created to support the IT security policy. The purpose of the standard is to define minimum requirements for each agency's information technology security management program. The IT security standard adopts the underlying assumptions of security policy. The aim of the standard is to establish a baseline of security controls that meet the requirements of various laws, regulations and security policy.

The security standard is organized around nine components of the security policy. Each component describes in detail the requirements which are mandatory or programmatic activities for a specific area of the IT security program. It also provides examples which describe how the agencies may meet these requirements. The standard requires agencies to develop and implement the IT security program in a manner commensurate with sensitivity and risk.

The first component addressed in the standard is risk management. The *risk management* delineates the steps necessary to identify, analyze, prioritize, and mitigate risks that could compromise IT systems. It defines requirements for roles and responsibilities, system inventory, business impact analysis, sensitivity classification, risk assessment, audits, and risk response. The *IT contingency planning* provides the steps necessary to plan for and execute recovery and restoration of state IT systems and data in case of an adverse event. This component focuses on continuity of operations planning, disaster recovery planning, and IT system backup and restoration.

The *IT systems security* requirements address how to protect IT systems through systems hardening, interoperability security, malicious code protection, and systems development lifecycle. The *logical access control* requirements provide necessary steps to protect IT systems and data by verifying and validating users to access IT systems and data. This can be achieved through account management, password management, and remote access. The *data protection* requirements address protection of data from improper or unauthorized disclosure. The focus here is on data storage media protection, and encryption. The *facilities security* requirements identify the steps necessary to safeguard the physical facilities that house IT equipment, systems, services, and personnel.

The *personnel security* requires restricting to those individuals who require such access as part of their job duties. Such an effort involves access determination and control, security awareness and training, and acceptable use. The *threat management* lists the steps necessary to protect IT systems and data by preparing for and responding to IT security incidents. This component addresses threat detection, incident handling, security monitoring and logging. Finally, the *IT asset management* outlines steps necessary to manage IT assets in a planned, organized, and secure fashion. The focus of this component is on IT asset control, software license management, and configuration management.

All these components have been reorganized from a larger set of thirteen components as described in the older security standard that was effective since 2001. The purpose of the older security standard (2001 version) was to define minimum

requirements for a security program and to align security technology with the business needs of the state. It emphasized the need of involving top agency management for an effective security program. It is interesting that business continuity planning was not part of the security program as reflected by the thirteen components. However, the standard recognized the critical impact of disruption of business on sensitive information and recommended that this be part of security planning.

Information systems security guidelines

The security guidelines describe methodologies that may be used to implement various requirements of the security policy and standard. For every component of the security standard, there is a corresponding guideline on the procedures required for compliance. Agencies are not required to follow the guidelines; however, these actually provide information on how to operationalize the standard. By the end of 2006, the ITA was still developing guidelines to support the security standard. The draft versions of five guidelines were uploaded on an online document system to obtain comments from various customer agencies. This essentially meant that agencies could use these draft versions to achieve compliance with the security policy and standard. However, the guidelines were not fully endorsed by the ITA since the documents were considered draft versions.

All supporting guidelines have been developed with a focus on educating users about information security. This is consistent with the approach advocated by CISO who believes that policy, standard and guidelines need to educate users on security as

well. As such, these guidelines provide general information on various concepts. Unfortunately, the balance has tilted towards providing more information on different security concepts rather than be clear on providing directives to users regarding how to achieve the objective of the guidelines. The summary and analysis of security guidelines developed by the ITA security department are presented next.

IT Logical Access Control guideline

The standard defines logical access control requirements in the areas of account management, password management and remote access. For account management, the guideline defines identification, authorization and authentication of various accounts. It also addresses the criteria to be used while processing various access requests. These include principles of least privilege and role-based access control. In addressing remote access, the guideline concentrates on encryption techniques and service hardening. The latter concept basically implies that the remote access services need to be secured both physically and logically.

The guideline failed to clearly articulate that an effective access control requires three levels of support: authorization, authentication, and monitoring. The guideline requires an explicit section on the assumptions, principles or objectives that are adopted or followed. However, this section needs to include the principles like default deny, least privilege, and need-to-know to be followed. This section should also indicate that role-based access control (RAC) has been adopted. Currently, RAC is listed under Account Management. Further, the access rights need to be aligned with the adopted

classification scheme (eg, top secret, secret, confidential). The current guideline does not recognize the importance of maintaining access rights through organizational changes. The guideline should also address controls for mobile and telecommuting aspects of business based on a risk assessment of each. Further, the guideline is silent on the issue of monitoring which should include details on reviews and audits of logs (for instance, what, who, how and timeframe involved).

IT Security Threat Management guideline

The IT security threat management guideline addresses threat detection, incident management, and monitoring and logging to minimize security risks. For threat detection, the focus is on intrusion detection and prevention practices. The goal of the threat detection process is to lower the difference in mean time between when an attack occurs and when responsible agency individuals becomes aware of an issue. Incident management details the activities required to investigate and to respond to detect security attacks on the organizational IT infrastructure. The aim is to minimize the impact and duration of security incidents. The final section describes the activities important for achieving an effective monitoring and logging of incidents. It provides information on system logging design, event log monitoring and correlation, and possible use of data mining techniques. For all these components the guideline clearly defines the roles and responsibilities of different stakeholders.

A review of the guideline indicates that there is no need for this guideline. The elements of this guideline should be captured in Risk Management, Logical Access

Control and Business Continuity Planning guidelines. Instead of having a separate Threat Management guideline it seems to make more sense to merge the portions of this guideline with other relevant guidelines. For instance, the Threat Detection section from this guideline could be merged and addressed under the Risk Management guideline. The Incident Handling section should be addressed under the Business Continuity Planning guideline. This would also reduce confusion among users in terms of expectations and their responsibilities.

IT Contingency Planning guideline

As per the guideline, the aim is to identify, exercise and review the actions necessary to restore and recover IT systems and data that support essential business functions. This is done by recommending methodologies to develop IT components of the Continuity of Operations Plan (COOP), the IT Disaster Recovery Plan, and the IT Systems Backup and Restoration plan. These plans would assist in recovering any IT systems or data that may have been rendered unavailable because of an unplanned security event. The guideline also emphasizes the need for regular exercises which test the plan in its entirety.

The review of this guideline indicates some concerns with the lack of clarity in its suggestions for contingency planning. Also, the guideline does not cover the subject area adequately. The IT contingency planning guideline should address the issues associated with assessment, plan, maintenance and teams. The assessment section could include risk assessment and business impact analysis. The next section of the plan might

provide information on preparation, response, resumption, recovery and restoration of business. The maintenance section should explain the testing, review, and audit requirements. Finally, the roles and responsibilities of various teams need to be clearly articulated.

Data Protection guideline

This guideline lists data protection practices that include roles and responsibilities, relationship to agency privacy policies, what must be protected, data storage media protection practices and data encryption practices. The guideline provides information on sensitive data and various risks to data. It then addresses different precautions required for storage and transmission of sensitive data. There is clear differentiation of responsibilities between data owner and custodian. The section on data storage media protection details the requirements for mobile data storage, authorization, disposal and re-use of such media.

The overall concern here should be with data integrity issues. The use of ‘CIA’ triad in the document is too prominent and repetitive. These principles are applicable to technical information systems. However, not all situations require confidentiality, integrity and availability. The current guideline may be improved by reorganizing it to address data sensitivity, data backup, data storage, and data protection mechanisms. A data sensitivity section should address data classification, risks to data and data losses. The section on data backup should detail appropriate policies and procedures. The storage of data must address both regular media and mobile media. Encryption

techniques may be discussed under the data protection mechanism section. This section would also include other mechanisms necessary to achieve the required level of data security.

IT System Security guideline

This guideline is structured around the directives of the state security policy. The security policy defines the area of focus for IT systems security to be IT systems hardening, IT systems interoperability security, malicious code protection, and IT systems development life cycle security. The logic behind the identification of these areas is not clear. For instance, malicious code protection is separately addressed in addition to IT systems hardening. Then again, various protection mechanisms available like encryption and intrusion detection systems have not been discussed.

In its current form, the guideline needs to take into consideration logical access control, data protection, threat management and IT asset management guidelines so as to minimize any repetition of controls and issues already addressed. Also, the issues covered under systems interoperability security seem to have been addressed in other guidelines. The guideline should be broadly organized to have sections on systems development and systems maintenance. The latter would provide required controls necessary to ensure security of existent systems. IT systems hardening and network architecture could be potential topics discussed in this section. The former would provide details about how to incorporate security into systems while they are under development.

Personnel security guideline

All the components addressed in this guideline are relevant to the subject matter. However, the effectiveness of the guideline could have been further enhanced. A new component on security incident reporting by personnel is required in the guideline. This section may address the issue of training users for incident recognition and reporting mechanisms. It is important that users are able to quickly communicate any suspicious activity to the right authorities. Also missing in the guideline is a statement on disciplinary action in case of any violations. This might have been captured in the security policy however it needs to be provided in the guideline as well. In its current form, the guideline does not emphasize security education, awareness and training programs in agencies. All these activities should be done on an on-going basis. The agencies need to understand the significance of awareness and training.

IT Security Audit guideline

The guideline does not clearly articulate the role and purpose of an IT security audit. The document fails to provide an adequate explanation of an IT security audit and why these are important. For instance, we might state the need for assessing the adequacy of organizational standards, or whether they help mitigate risks to an organization. The document does not emphasize that the audit basically reflects an organization's risk management posture, as well as its policies and standards that must be followed. Such an audit checks whether security controls are mitigating risks to an

organization. An audit should be based on an organization's objectives and risk priorities. Further, the document does not clearly state the importance of establishing an audit baseline. One may use the existing standard in its entirety for such a purpose.

As of July 2007, the ITA was still in the process of developing the IT asset management guideline and facilities security guideline.

Information assurance and compliance program

In addition to the security policy, standard and guidelines, the security program at the ITA involves an information assurance program and a compliance program. These have been developed in response to an audit conducted by the state. The ITA was directed to develop an action plan in response to recommendations of the audit report. However, there was no comprehensive approach developed to achieve an integrated program. Rather, the program developed in an emergent fashion. CISO decided on the issues that required immediate attention. As the security department started working on these components, other aspects of the program emerged that needed to be addressed as well. These aspects made sense so as to achieve an effective security program. Partly, these newer aspects emerged as the security department interacted with different agencies and tried to understand their security needs and compliance with different regulations. Each of these components of the security program are discussed in this section.

Information assurance program

The aim of the information assurance program at the ITA is to perform security analyses of sensitive IT systems in terms of appropriate security controls. The ITA has the responsibility for providing a secure IT infrastructure that also encompasses various regulations and laws, both state and federal, as applicable. The security department must collect information, including IT security audit plans, on each sensitive system so as to conduct the analysis. A template was provided to 63 agencies in order to capture the required information. In addition, a technical data survey captured information on servers (logical and physical), infrastructure and network devices, and environmental and physical controls.

Based on the information from agencies, an analysis would be performed by the ITA to assess the security controls in place. Such analysis would identify various gaps and provide recommendations on appropriate security controls required. In case of inadequate security controls, the ITA would develop a working plan with necessary corrective actions to be implemented. This would also take into account the risk assessment and corresponding adjustments to risk management. In the end, the ITA would issue a letter of assurance to each agency notifying of the results of the security analysis. To facilitate the process of information assurance, the security department has initiated development of a security data warehouse. The goal is to provide customer agencies with online access to update security information in the database. The security analysis of sensitive systems at different agencies will be conducted on an annual basis by the ITA security department.

Compliance program

The monitoring and enforcement of the security policy and standard has to be continuous so as to assure effectiveness of different protection measures. The security directorate would evaluate compliance through the use of audits, management reviews, self-assessments, surveys, and other informal indicators. A combination of these measures would be used to achieve greater reliability of results. Each agency is also required to designate an ISO and a backup ISO. In addition, agencies must perform business impact analyses and exercise contingency plans. That is, agencies need to be prepared for response to IT security incidents. All IT systems and data need to be inventoried and classified. A thorough risk assessment and IT security audit of sensitive systems is also required by the security directorate. The security requirements are to be incorporated in SDLC of IT applications. The security configuration standards are also to be implemented. Appropriate data protection practices will be defined and formal account management practices documented. The agencies need to establish access control, security awareness training and acceptable use policies for personnel security. Finally, it is imperative to safeguard the physical facilities.

4.2.3 Process

The state legislation requires all government agencies to comply with the state IT security policy and standard. In addition, the state required assessment of information security controls at agencies by state auditors. The security program so

developed is in reaction to the security audit. Around December 2006, the audit report was presented in state assembly and legislators required the security directorate at the ITA to address all its recommendations. Overall, the report provided four recommendations to improve the state of security at Wonderland. Based on recommendations of the security audit report, the officers of the security department formulated an action plan to achieve the desired security objectives. The security program so developed is not the product of well planned or thought out processes. Rather, it is reactionary in nature. The executives at the security department worked first on the security policy and standard because of legislative mandates. Once these were developed, the directorate started working on the guidelines.

The organizational structure of the ITA security services department reflected the prior security program. The security department was broadly divided into six divisions including standards, policies and procedures, secure infrastructure and technical support, critical infrastructure protection and service continuity, risk management, information security training and awareness and, incident management. Each of these divisions was responsible for specific components of the security program. Post audit report, the organizational structure of the security services department reflects the inherent changes based on the recommendations of the report. The most significant change is the emergence of a security assurance division. This division, along with standards and guidelines promotes information security in the state.

In response to the first recommendation of the audit report, the action plan developed by the security services department involved analysis of audit data to define

areas of need, identify communication vehicles, promote information security, and comply with the state information security standard. Based on the security domains from the security assessment report, the top-five areas of need were SDLC security, software change management, monitoring and logging, standard configuration, and security awareness and training. To promote information security, the security department is expending its efforts on the development of standards and guidelines, configuration standards, and an information assurance program. The assurance program involves collecting information and performing IT security audits on sensitive systems. It further involves analyzing current security controls and documenting any gaps. The purpose of the program is to provide assurance that the IT infrastructure of agencies has sufficient safeguards in place to protect information and databases.

Each individual in charge is responsible for developing that particular security component. The developmental efforts of the division must incorporate requirements from the security policy and standard, as well as, the audit report. Such initiatives must ensure that various activities of the division result in achievement of security objectives set forth by the state. The scope of these divisions includes the ITA and other government agencies. It is the responsibility of various divisions of security services department to provide assistance and expertise to agencies as they develop their information security programs. Each individual in-charge of a division works in consultation with the Deputy CISO and CISO to identify specific initiatives of the division. The finer details of these initiatives are hammered out by division members with the assistance of consultants. The process involved for developing security

initiatives might differ between divisions; however, the general nature of development remains the same. Ultimately, the CISO must approve various initiatives before any work is undertaken. In addition to email and face-to-face meetings, various tasks are assigned by the CISO at the bi-monthly staff meetings. The staff meetings also provide a forum to get updates and status reports of various projects.

Let us now take a look at the operations of the Standards, Policies and Procedures division of the security services department. The process followed by other divisions will be briefly described afterwards.

Security policy, standard and guideline review process

The policy, standard and guidelines review process is described in this section. The subject area in-charge writes the document, which is then reviewed by the security manager who provides suggestions or comments. Then, initial feedback or comments are sought from one or two stakeholders. The revised document is given to management (CISO, deputy CISO) for comments. The document is then sent to an internal policy expert and his team for review. It is then sent back to the security management for approval. Upon approval, the document is uploaded on an online document system for about one month for comments from all state agencies. Then, the review committee meets to discuss any comments. The revised document goes back to the security management for further comments. The final document is sent to the Secretary of Technology, the Governor, and the State legislature for approval or enactment. In

general, policy, standard and guideline documents undergo four to twelve revisions before getting finally approved.

During review committee meetings, the members sequentially review comments from online document system. The comments received from agencies through the online document system generally address minor issues. Occasionally, there are a few interesting comments. The comments are not filtered for the review meeting but rather all comments are discussed. A consultant reads each comment and provides her perspective. Then, the floor is open for the rest of the committee to comment. If there is disagreement, the viewpoint of the ITA security member is final. The aim is to generate consensus among the group. Even if there is only one member who has an issue or different perspective, this issue is heard, analyzed and deliberated. If it deserves even little bit of merit, her suggestions are included. Disagreements are common.

While consultants generally try to rush up through the comments however, the ITA team consistently deliberates each comment. They try to understand and identify ways in which other readers might misunderstand or misconstrue the statement that raised the discussion. These members do bring their past experience in government agencies to enlighten the current problem. They are able to fall back on their experience in various agencies and develop statements that would be consistent with the ground realities and user habits in those agencies. The members are flexible enough to take a radical or fresh view which might be better than their view or consideration. The endeavor seems to be on developing the best and most appropriate guidelines.

There is constant struggle during meetings about the objectives of the guideline as to what they are trying to achieve. For instance, the members question whether the concerns need to be addressed at the business level or the IT level. Another instance involves whether to have emphasis on user education or to simply stipulate what needs to be done. In case of disagreements, the consultant suggests a language that catches the disagreeing member's sentiments and is at the same time agreeable to the rest of the members. In other words, the meetings include a considerable amount of negotiations. If major changes are incorporated, the document needs to go through another round of revision from agencies. The decision regarding another review process is made by a group of internal policy experts at the ITA.

Information assurance process

The focus of the assurance program seems to be on compliance. The emphasis is on checking whether rules have been followed and documented for cases when the standard is not followed. There might be cases where rules cannot be followed thoroughly. Such cases need to be documented and new rules specified. It is also important to identify mitigating mechanisms. The group relies upon state security policy and other mandates such as HIPPA or IRS rules provided by agencies. The group is mainly concerned with the Outsourcing Firm as IT infrastructure providing organization. The group has to evaluate weaknesses in infrastructure that might have an impact on ITA's operations.

For the assurance process, templates were developed for different agencies. In terms of reaching out, the group used email, SAG meetings and developed a data warehouse. The purpose of the data warehouse was to help identify problems. The data warehouse spreads over domains of technical and audit plan information. One of the issues that the group is facing with the data warehouse development is that plans, phases and processes are constantly changing. This has led to significant delays in the development of this project. Essentially, the data warehouse has been created to collect remediation plans from agencies. The agencies are expected to provide information on sensitive data. They have to identify and submit audit plan for sensitive systems. Then, the result of the audit must be reported to the ITA. If there are any weaknesses identified, the security group requires agencies to submit appropriate remediation plans. The warehouse also assists in capturing associated roles and responsibilities within an agency.

The security group realizes that they do not have resources to help every agency. The hope is that as the department grows, assurance teams can be sent to various agencies in order to help them out. The group would also like to conduct an annual audit of twenty-five large agencies. In terms of issues, the group has observed the lack of expertise in smaller agencies. Another impediment has been the relatively large number of systems that need to be audited. Big agencies appreciate an audit; however, smaller ones do not. But the group realizes that they have to conduct audits of all processes and systems. Lack of support from agencies is an issue.

In order to overcome the problem of withholding information, the group constantly adjusts questions and asks for elaboration. This is to overcome the problem that some agencies withhold information to protect themselves if the questions are not specific enough. The group is striving to reach a position where it can assign grades to agencies on their assurance level. However, such an effort has its own issues. The grades can in fact be a reflection on the security group at the ITA. This is because the ITA owns the systems and infrastructure while agencies own only the data. This is the kind of fuzziness involved as a result of IT consolidation endeavors in the state.

Awareness and training

The ITA security department identified training as a major activity in the security program formulation process. There is recognition of the human role in security problems of organizations, which points to the significance of an awareness program about information security issues to prevent or detect security problems. The awareness training at the ITA is to focus on executives, policy makers, program and functional managers, security and audit personnel, computer management and operations, and end users. Such training can be disseminated through existing policy and procedures manuals, written materials, presentations and classes, and audio-visual training programs. The aim of training is to create an awareness of security risks and the importance of appropriate safeguards, while emphasizing specific responsibilities of each stakeholder. Another effort involves providing information about the security program through the orientation for new ISOs. During such orientations, new ISO of an

agency is educated about necessity for good security in an organization and the security program developed by ITA.

Communication vehicles

To achieve the objectives of the security program, the ITA realized the importance of communicating effectively with the different stakeholder agencies. These communication vehicles include meetings, councils and various communiqués. One of the prominent mediums used for communication with agencies is the monthly meeting of the Security Advisory Group (SAG). These meetings are attended by ISOs of all agencies either physically or remotely through telecommunication technology. In addition, there are IT Resource (ITR) meetings which are mandated by regulation where IT requirements of the various agencies is discussed. Finally, there is communiqué from the CIO via email and other email communication from the Governor's office informing about the current state of security. These vehicles could also be used to indicate support of management at the highest level in the state.

A new initiative by the security department at ITA is the formation of a Security Council. The members of this council are the representatives of politically heavyweight agencies and also those organizations that have been able to achieve some level of success with security efforts. The underlying aim is to be productive in terms of security. This council provides guidance to the security department on what to do, how to improve the security program, and how to make the SAG meetings more beneficial

for agencies. To gauge customer satisfaction, another council has been formed which involves only customer agencies of the ITA.

4.3 Department of Transportation

The Department of Transportation (DOT) is a state transportation agency located in the southeastern part of the US. It maintains one of the largest state-maintained highway systems in the nation with approximately sixty thousand miles of roadway and twenty thousand bridges. The DOT is responsible for building, maintaining and operating the state's roads, bridges and tunnels. It also provides funding for airports, seaports, rail and public transportation. The DOT employs around eight thousand and eight hundred full time organizational members, along with additional part-time employees and contractors. The DOT is a multi-million dollar business that transcends engineering and construction areas. The organization has been known for transportation excellence for over hundred years and is also the largest landowner in the state of Wonderland. The context, content and process of information system security initiatives at DOT are described in the rest of this section.

4.3.1 Context

The DOT defines its mission as to plan, develop, deliver, operate and maintain, on time and on budget, the best possible transportation system for the citizens of the state. Towards this end, it has to design network to meet future needs and also provide the engineering and financial expertise to construct the project. The DOT is also

responsible to manage the operation of a safe, effective and efficient ground transportation system. The DOT has clearly defined values that it expects all organizational members to abide by. These values include safety and security; truth, trust and teamwork; environmental excellence; action and accountability; and, results and respect. The ongoing emphasis of the organization is on innovation and improvement to become 21st century transportation mobility agency.

Regulatory environment

As a government agency, the DOT is regulated by the state legislations and statutes, and is accountable to the state citizens. In terms of information systems security, the DOT has to abide by the state legislation which requires compliance with the state security policy and standard. The legislation mandates the head of each agency to inform the state technology agency of any known security incident within twenty-four hours of discovery. Further, the head of each agency would be held accountable for any security incident in that organization. The Secretary of Technology has been empowered to ensure compliance with the state security policy and standard across Wonderland.

Competitive environment

The DOT is a government agency responsible for the transportation needs of the state citizens. The DOT has a total annual budget of about four billion dollars with forty percent of the budget allocated to highway maintenance and twenty-five percent

assigned for highway systems construction. One quarter of the budget is funded through the federal sources, while the rest is generated by the state. Due to increased costs and lack of funding, the DOT's six-year plan for transportation improvement was reduced in 2002 from ten billion dollars to about four billion dollars. As a result, the focus of the organization shifted to deliver projects on time and on budget along with maintaining high quality. The management structure was streamlined to ensure effective decision-making authority whereby accountability was shifted from central office to the field.

Since 2002, the endeavor for efficiency has helped DOT achieve an annual cost reduction of about a quarter billion dollar. More than eighty percent of the projects are delivered on time and within budget as compared to half the projects completed within budget and only one-thirds delivered on time since the accountability efforts began. In addition, significant savings has also been achieved through outsourcing and reducing organizational size. The DOT has utilized public-private partnership that encourages private companies to build and operate roads and other transportation services. The organization has collaborated with private sector to find new ways to help fund and deliver projects. This has resulted in construction projects valuing more than eleven billion dollars.

As a consequence of non-availability of dedicated funding, the DOT shifted its focus from construction to achieving operational efficiency. The organization realized the issue was efficient flow of traffic and simply building more roads was no longer a viable solution. The change in perspective pushed the organization to seek solutions through technology. Now, the DOT takes pride in becoming a leading technology savvy

government agency. In order to become more transparent, a web-based performance measurement system was developed to provide customers a real-time snapshot of DOT's projects in terms of time and budget. A newer version of this system aims to broaden the scope to show latest performance of all business areas including road maintenance, plans, studies, safety, finances, operations and environmental compliance.

The DOT has also developed the Smart Traffic Centers across the state that utilizes technology to consolidate different functions in order to improve traffic flow and traveler information. A statewide phone system has been developed to provide real-time traffic information to the motorists. In order to improve operational efficiency, a Project Cost Estimation System has been developed that allows DOT to obtain accurate project forecasts. It also implemented an Asset Management System that tracks asset conditions.

A utilities management system has been developed that provides current updated status of highway projects. The consistent emphasis is on developing intelligent transportation systems. The electronic toll collection has been improved through secure tags. The DOT has also invested heavily in sophisticated geographic information systems.

In order to retain knowledge because of brain drain, the DOT has established a knowledge management program to capture and preserve knowledge of the most experienced employees. The system allows preserving institutional and employee knowledge. It creates and fosters internal networks of experts on a subject to promote efficiency and to ensure consistency of best practices throughout the organization. DOT also created an automated information management system to ensure requests for

records and data consistent with the Freedom of Information Act are responded to quickly and accurately. The development and maintenance of all these IT applications and systems are done in-house at the IT division. The emphasis so far has been on innovation and integration of technology with business operations at the DOT. The aim is to achieve improved transportation program through the use of technology.

Organizational structure

The Transportation Commissioner is at the helm of DOT's organizational structure. This position is a political appointment with appointees nominated by the Governor. The Commissioner is not actively involved with the business operations of the DOT. The position of Commissioner is more symbolic and the role is to guide the organization in transforming the Governor's vision. The Transportation Board serves as an oversight for the Commissioner's position and the role is similar to that of a board of directors in a non-government organization. The State Secretary of Technology serves as the chairman of this board. The members of the board are appointed by the Governor and approved by the General Assembly. The Deputy Commissioner is responsible for the day-to-day business operations at the DOT (figure 4.3). This position is equivalent of a Chief Executive Officer (CEO) position in a non-government organization. Individuals for this position are generally promoted from within the organization. It is an active appointment.

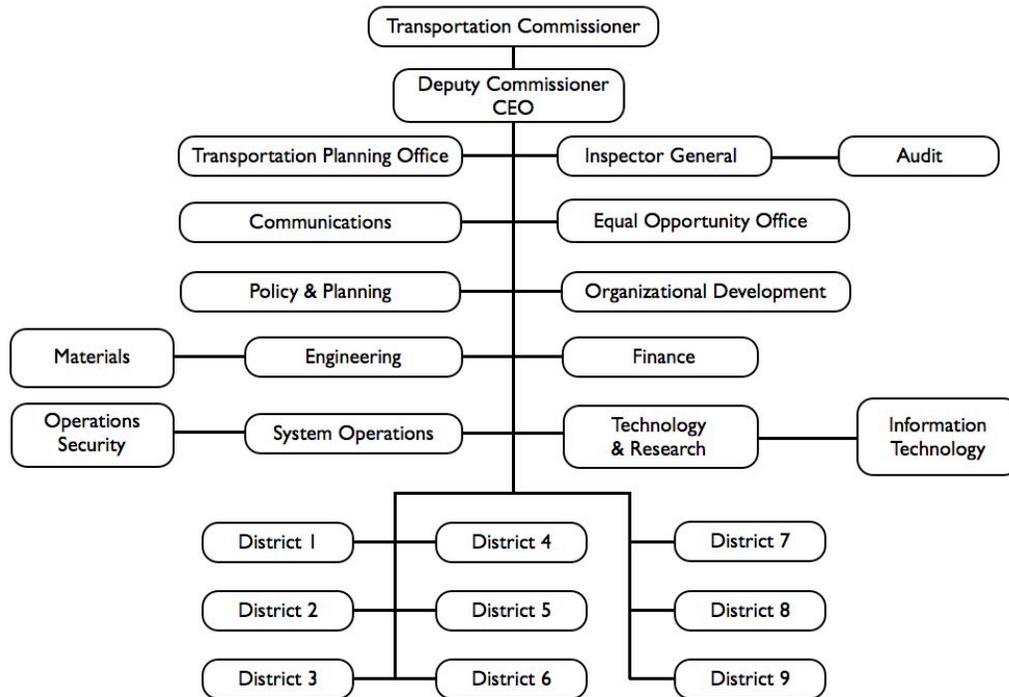


Figure 4.3: Organizational structure of the Department of Transportation

As an organization, DOT is broadly structured as divisions and districts. For highway operations, the state of Wonderland is divided into nine districts headed by a District Administrator. Each district is responsible for the maintenance, construction and operations of transportation projects for that particular region. The central office is divided into ten core areas that are officially headed by a Chief. An organizational member who has demonstrated competence in the specific area occupies this position. Each core area is further divided into divisions. There are approximately thirty divisions, which essentially serve as operational and administrative units at the DOT.

The Information Technology Division is placed under the Technology & Research in the organizational structure. This division is led by the Chief Information Officer (CIO) and is responsible for all the IT needs of DOT. The division is structured into five units with a manager in-charge of each unit. The units basically involve applications development, systems engineering, and IT governance. The IT division also houses a unit operated by the state technology agency to provide necessary technological infrastructure support to ensure smooth operations. This is essentially a result of statewide IT consolidation initiative. The information security program at DOT is placed under the IT Governance unit (figure 4.4).

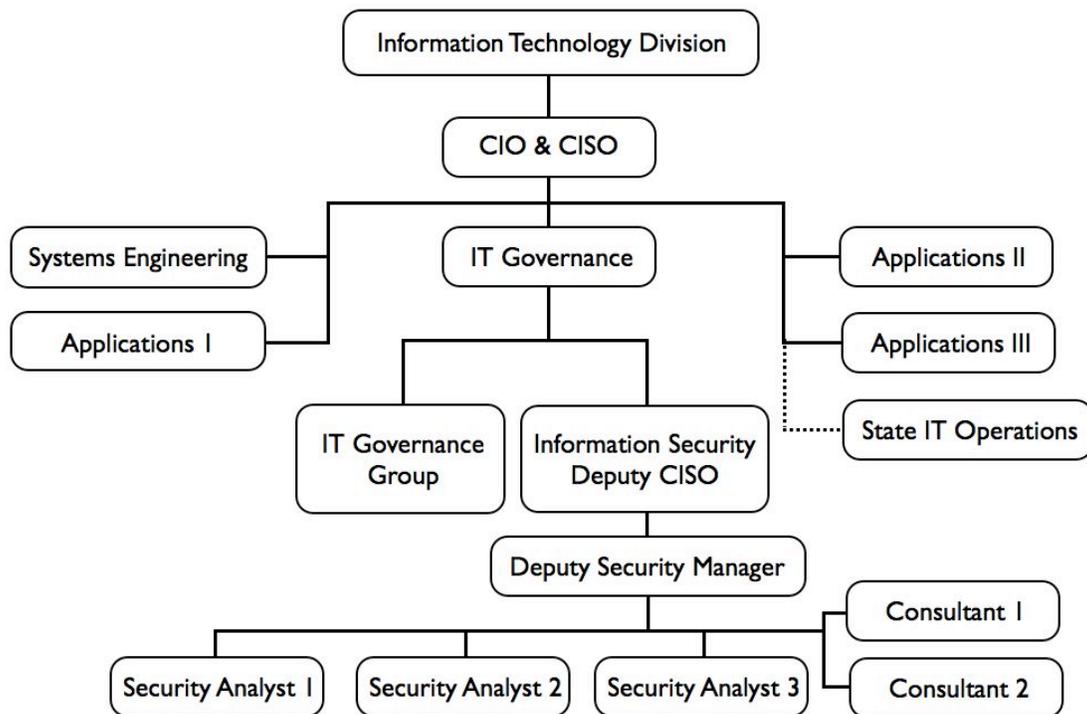


Figure 4.4: Information security department of the Department of Transportation

The CIO decided to take on the position of the CISO as an additional responsibility. A manager has been appointed to run the security operations, who also serves as the designated Deputy CISO. This presents an interesting situation as the Deputy CISO is technically supposed to report directly to the CISO; however, the security operations have been placed under supervision of the IT Governance Manager in the organizational structure. The information security program is handled by two executive officers, three security analysts and two consultants. These individuals are responsible for the development, implementation and maintenance of the program. However, the CISO is ultimately responsible for the security program and held accountable in case of any adverse event.

4.3.2 Content

The security department at DOT adopted the state information systems security policy in its entirety. The group also decided to follow the prescribed state security standard and supporting guidelines. The details of the state security policy, standard and guidelines, along with the security program are provided in section 4.2.2. In addition, the group decided to develop a security program manual for internal operations at the DOT. In essence, the security department members reconfigured the state prescribed security policy and standard in the context of DOT business environment. For each component, the group detailed exact responsibilities and procedures as applicable for DOT in order to ensure necessary security requirements.

The security program manual represents details of how DOT will manage adherence to the state security policy and standards. The manual's parallelism with the state security policy extends to the level of each itemized component identical to the component in the security standard. For each component, an office of primary responsibility is assigned, which is responsible for defining requirements, overall management, and implementation of processes and procedures associated with the component. In addition, compliance validation for each component is also provided, which identifies the means by which effectiveness of the processes can be monitored and measured. The manual is structured along nine components as outlined by the state security policy. The description of each of the component areas is briefly described in this section.

For *risk management*, well-defined processes need to be implemented that would minimize the effect of threats to IT system assets. This would involve establishing formal roles and assign responsibilities to manage and protect the security of IT systems. A business impact analysis must be used to identify business functions that are essential to DOT's mission. In addition, IT systems, applications and data need to be classified by the systems and data owners according to their sensitivity with respect to an unauthorized disclosure, modification and sensitivity to outages. Risk assessment may be used to determine the likelihood of the threat's occurrence, evaluate the potential loss or threat, assign a criticality and identify mitigation and recovery strategies. Finally, a security audit needs to be conducted to examine IT systems policies, records and activities.

The *threat management* component defines the requirements for processes to be implemented by service providers to prepare for and respond to the IT security incidents. An intrusion detection and prevention must be implemented. Adequate response to suspected or known breaches of IT security safeguards needs to be identified. Also, procedures need to be specified so as to effectively monitor and record IT systems and application activity. The *IT asset management* defines the procedures to protect its IT systems, applications, data and equipment in a planned, organized, and secure fashion. DOT is to adopt configuration management to provide a logical model of the IT infrastructure by identifying, maintaining and verifying the version of all configuration items. The *contingency planning* component defines requirements and processes needed to recover and restore IT systems, applications, and data that support essential business functions. The COOP plan identifies the steps necessary to provide continuity for such functions. The restoration of mission-critical IT systems and applications is necessary to support essential business functions. Such procedures form the basis of disaster recovery plan.

The *IT systems security* specifies DOT's requirements for securing IT assets. In order to do so, technical security controls are necessary to protect the DOT systems against vulnerabilities. Interoperability security identifies the steps necessary to protect data shared between the IT systems and applications from damage caused by malicious code. Finally, the security-related processes must be defined during each phase of the development life cycle for the protection of the DOT application systems. The component of *data protection* details the processes and procedures necessary to validate

protection of data from improper or unauthorized access or disclosure. Data needs to be protected whether it resides or travels through the DOT IT systems and applications. In order to protect sensitive data, a framework would be provided for selecting and implementing encryption controls.

The *logical access control* outlines the process to validate that users are who they say they are and that they are permitted to use IT system's assets of the DOT. It is imperative to identify the steps necessary for requesting, granting, administering, and terminating accounts and access to the DOT computer application and data. Also, continued verification processes are necessary for password management by the DOT's employees and the IT service providers to protect IT assets. In terms of remote access, the steps necessary to provide for the secure use of remote access within the IT network need to be identified.

The *facilities security* is concerned with protection of physical facilities that house IT equipment, computers, systems, services, and personnel of the DOT. The Security Operations department and Critical Infrastructure Protection department are responsible for identifying necessary processes and procedures. The *personnel security* component provides requirements that are necessary for restricting access to IT assets to only those individuals who require such access as part of their job duties. This component is also responsible for the logical and physical access determination and control mechanisms. Also, organizational members need to be made aware of system security requirements and their responsibilities to protect IT assets of the DOT.

4.3.3 Process

The process of implementing the information security initiatives at DOT is described in this section.

Risk management

The security group conducted classification of systems and performed risk assessment as part of the process for risk management. The group emphasizes the need for risk assessment of IT systems that are critical to operations. In general, the systems are the responsibility of the systems owners but the security department decided to enforce standard procedures across these systems. The department established and documented procedures for those areas that are covered by the IT security manual. The technology owner is in charge but the security group felt that a tool was needed to capture information and therefore, decided to have a team member work with the users. Such an approach is to help the users and train them on classifying sensitive systems.

The last assessment conducted by the group was on behalf of the ITA on cyber security. It was agency-wide review and the focus was on agency rather than applications. Technically, the security group was not able to get compliant or perform all risk assessments by the deadline; however, plans were in place and assessments were ongoing. The security group re-conducted the BIA as the business needs had changed. The group members also conducted data classification as per new criteria and reassessed all systems for sensitivity.

Contingency planning

The COOP entails developing manual operations in case the IT operations are unavailable. Although addressed under the IT security manual, the COOP component of the security program is not under the IT department at DOT but rather the Operations Security department (OS). This department manages the program and coordinates COOP activities of nine districts at the DOT. This was done as COOP was considered to have different requirements than IT. Further, it did make sense to assign COOP to a group that does not have political authority. The IT department does not dictate policies and hence should not have responsibility to ensure COOP. The management decided to follow industry practice which states that COOP should be located in the operations department.

With the new state requirement, the department is integrating IT security requirements in COOP. This was not done earlier as IT was contracted out. The integration is carried out across all nine districts and there is some internal alignment going on. In past four years, the DOT is moving rapidly towards operations based approach. The Division Heads have assigned a COOP coordinator in all divisions at the central office. These COOP coordinators regularly meet with the OS department members to discuss changes. For COOP there are three tiers. Tier 1 is ascribed to the systems and processes that need two days to be restored to normal operations. Tier 2 implies that the systems can wait a week before restoring, while tier 3 is assigned to not so serious systems.

Preparedness has become core issue for all agencies. In terms of day-to-day operations, one does not think about COOP on regular basis. To address such concerns, the group has emphasized the need for organizational members to know about COOP. For latter, the department has created awareness initiatives. For instance, the month of September is earmarked as the preparedness month and various informative displays are put across the central office. The OS department also has an online repository for COOP literature. The group has also sought support of the top management. The problem encountered by the group is that the government agencies generally do not do things till law requires them to.

Another concern is protecting access from unauthorized users. The problem is that with an increase in numbers drastically the security might be relaxed. For example, if there is pandemic flu, buildings are here but people are not. In such an event, people are working from home. The current policy says that one can only access the state IT network with a state machine. This might be problematic as people would not be able to access the systems. As such, the ITA is planning to relax security and extend the policy to be applicable for personal machines as well.

Disaster recovery

In case of disaster recovery, the security group found that the procedures were not documented properly. The group also realized that the procedures were not being tested properly either. As a result, the security members started to document all procedures. The aim was to put together an organization with good communication

procedures. The group was focused on establishing different steps required in place for various components of the security program.

Data protection

The security group conducted data classification and performed sensitivity analysis. For hard disk retiring, the security group members focused on understanding the processes. The effort required cooperation from organizational members where they would report back to the security group. The security group members also realized the importance to go to vendor and conduct spot checks to see whether data was dealt with appropriately. For such an effort, the group realized the need to develop forensic expertise. Such plans were postponed for the time because of the lack of adequate resources. For the earlier half of the year, the group was getting procedures, documents, and reports. Now, the security process is ongoing and in an operational mode.

Account management

At DOT, there were number of different methods to request access to the IT systems. The security department members worked on the problem to get standard forms for request. The members decided to address the problem in three phases. For the first phase, the need to have standard process for access was determined. Next step involved making standard request forms available. Finally, the members realized the practicality of the process to be automated for web-based access. The latter effort was ongoing at the time the researcher left the field site.

Intrusion detection

The security policy ascertains the responsibility of monitoring and log to respective agencies. The DOT did not have this responsibility because the agency was no longer owner of the IT infrastructure. The security department at DOT had to communicate with the ITA on this aspect. The ITA responded that they did not have an intrusion detection system at the moment and as such, there were no associated logs. The problems that the group felt was the lack of control over the ITA in order to get them do what is required. The IDS was supposed to be active but was not available. This required the security group at DOT to plan for the risk exposure due to the lack of an intrusion detection system.

Incident management

At DOT, there were procedural problems in the process of incident reporting and handling. The organization did not have a predefined channel to report IT security problems. The organizational members were not clear on whom to contact or what to do in case of an IT security emergency. In case of an incident, the members would end up contacting either the police or the CIO. A formal procedure for reporting incident was missing. As a result, a document outlining procedures for the district and division offices was developed detailing necessary steps required to ensure security as expected by the security department at DOT. The issue was whether the state technology agency needs to know about an incident. Subsequently, the process for detecting attacks against

the agency was streamlined. Basically, the aim was to reduce the time involved in reporting an incident. This was seen to be essential so that the DOT could get decent response time before the incident were to be notified to the state technology office.

In order to reduce time for quicker response, there was the need for a reporting system that all employees could access. Further, the department did not have a standard form for reporting incidents although need for such a form was clearly there. In fact, two incidents occurred before the department agreed on developing a standard form on the lines of one used by the state technology agency. In case of an incident, a user completes the incident form and submits it. This generates notification to be accessed by the security analysts and the security manager. Once an analyst gets an incident report, she is expected to gather relevant information, file and track the incident. Such process involves contacting respective district or division office where the incident has happened. From then on, the security analyst is expected to take the responsibility and determine the future course of action. The security department is expected to notify stakeholders at the DOT and also inform the state technology agency, which is responsible for technical security.

As follow up to an incident, the security department is required to keep records about the details of an incident, its status, and resolution in terms of particular steps taken to control or resolve the incident. Such information is also required for audit purposes. In terms of technical measures taken, the department relies upon the state technology agency to regularly forward reports pertaining to incidents occurred at the DOT on a monthly basis. However, the state technology agency does not have a system

to provide timely reports.

Awareness and Training

The department manages an online training program. Each new employee has to take this online certification within thirty days of joining the organization. The group has fine-tuned the security policies to meet the DOT requirements. The vendor updates the vault (where policy documents are stored) when there is any change in the policy. All employees of the DOT have to undergo an online security training and obtain a certification of compliance each year. Each employee has to read the IT security policy and answer few multiple-choice type questions pertaining to the security policy. At the end of successfully answering these questions, each user is awarded a certificate that records date of completion of the online training. The account access is generally terminated for employees who do not attain an online certification.

The security group created a website and developed a prominent position on the portal of the DOT for incident reporting, awareness training, security program manual, security policy, and cyber tips. For incident reporting link, the group posted documentation and incident forms. The portal provides an access form for new employees to be signed by the supervisor and is then forwarded to different data owners. Another form is used to remove users from all systems for which the manager has to initiate the process. The security group also provides monthly newsletters on incidents, education, and best practices. A brochure on useful security tips is distributed to all districts and divisions. The group also publishes weekly reports that

are forwarded to the top management. The report provides information on what person's are in non-compliance with security.

The security group felt the need to provide the security training manually and have awareness workshops. The group decided to conduct workshops for the officers of responsibility from each division. During the period of February to July 2007, the group conducted four awareness workshops although not on a regular interval. The participants for the workshops include the Information Security Coordinators and the District Administrator. The security executives inform the attendees about the security program and the need for such an endeavor. In fact, the awareness and training impacts all parts of the security process.

4.4 Discussion

The theory of contextualist strategic change has been used in this chapter as a theoretical framework to study two organizations. This theoretical framework has been used in the extant literature in a static sense. That is, various researchers have analyzed an organization using content, context and process components of the theoretical framework. However, such an approach is problematic. The static use informs us about what has been done in a particular case. It does not answer the 'why' element to allow richer analysis. The theory of contextualist strategic change provides a structure or framework that best serves as a meta-theory. The real intent or motivations of actors cannot be explicated without understanding or exploring the relationships between theoretical components of this framework. For instance, one may question why a

particular process or action was undertaken? Maybe it was done to account for contextual realities. The contextualist theoretical framework alone does not explain such questions adequately.

In essence, there is a need for a dynamic use of the theoretical framework. The contextualist theory in itself is limited in providing rich insight about ‘why’ things are being done as they are done. At the same time, the theory does not help us in unraveling ‘what’ are the reasons for embarking upon a certain path. The static use of the framework only answers ‘how’ aspects such as how things are currently conducted in a given situation. We can definitely analyze the situation as per the literature but such an approach again is not rich in analysis. The theory is indeed useful in identifying relevant areas for analysis, however the need to study subtle underlying relationships between the components is generally missed.

Pettigrew (1987) developed the theory of contextualist strategic change based upon Pepper’s (1970) world theory of contextualism. For contextualism, the social world is comprised of events and each given event has quality and texture. The quality of a given event is its intuited wholeness, while texture deals with the details and relations of an act that makeup its quality. The texture is made up of a strand and it lies in a context. The strand is the interconnection among details of an act, whereas context is the interconnection among strands. Here, the emphasis is on the intricate relationships between details of an act that form an event. In contextualism, the actual structure of an event is ultimately determined by its qualitative structure. As such, we need to pay attention to the relationships between the theoretical components of the theory of

contextualist strategic change. That is, it is imperative to study the links between context, content and processes.

In explaining the theory of contextualist strategic change, Pettigrew (1987) did mention the need to study the interconnections between context, content and process through time. Walsham (1993) indeed studied the link between context and process, while rest of the linkages was usefully assumed to be the content of an information system. However, the content of an information system can also be analyzed and indeed have implications for success with the subsequent implementation of an information system in an organization. In order to understand the subtle yet powerful relationships underlying the phenomenon of study we need to employ further excavating tools in the form of theoretical systems that would operate within the assumptions of the overall (meta) theoretical framework of the contextualist strategic change. Further, such theoretical systems to be employed to study the relationships should also be aligned with the ontological and epistemological position of the meta-theory.

4.5 Conclusion

In this chapter, the contextualist interpretation of case studies has been provided. The Information Technology Agency and the Department of Transportation have been analyzed in terms of the context, content and process components of the theoretical framework. The chapter has called for a dynamic use of the theory of contextualist strategic change rather than a static one. This is to emphasize the need to study the relationships between different components of the theoretical framework.

CHAPTER 5

Development of Strategic Information Systems Security Initiatives at Information Technology Agency

5.1 Introduction

In this chapter, Bourdieu's cultural theory is employed to understand introduction of information system security initiatives in an organization. A cultural perspective would be helpful in developing the content of an initiative with respect to the context of a given organization. In order to achieve desired security objectives it becomes imperative to use a theory that would be considerate in explaining the relationship between context and content. At the same time, an analysis of culture would also have to account for the interaction between content, context and process, as formulating the content involves managing the latter two respectively. Bourdieu's theory has been used here especially since it emphasizes the continuous (rather than change) orientations of culture in terms of reproducing the objective structures of social world and subjective dispositions of actors. The introduction of an initiative does not mean that such an initiative be divorced from an organization's rich context. But rather we should take advantage of the historical context. A proper understanding of the

cultural intent of the stakeholders would be helpful in creating opportune situations that are accommodating to institutionalization of information systems security initiatives in an organization.

This chapter is divided into nine sections. The next section describes Bourdieu's cultural theory. This is followed by the sections explicating field, habitus and capital in the case of ITA. Section 5.6 provides cultural analysis of various strategies pursued to attain actions at ITA. Section 5.7 presents the role symbolic forms play in establishing dominance in the social world. Section 5.8 identifies the key findings for discussion. The last section concludes the interpretation of information systems security initiative in an organization from a cultural perspective.

5.2 Bourdieu's Cultural Theory

Bourdieu's model of practices conceptualizes action as the outcome of the relationship between habitus, capital, and field (figure 5.1). It emerges from the encounter between the opportunities and constraints (objective structures) presented by situation and dispositions (subjective) of habitus. Field specifies power relation and hierarchy. These are the arenas of conflict and struggle over valued cultural resources. For habitus, actors are adapting to external constraints and establishing distinction from other competing actors. Practices cannot be attributed to either habitus or field but grows out of the inter-relationship between them. The relation of agency and structure is considered to be one of the main problems in social theory. Bourdieu approaches this issue as a dialectical relationship between agency and structure in order to transcend the

dichotomy. He does not agree with the position of considering human action as a direct result of either external or internal factors. Bourdieu integrates agency and structure by considering action as a function of culture, structure and power.

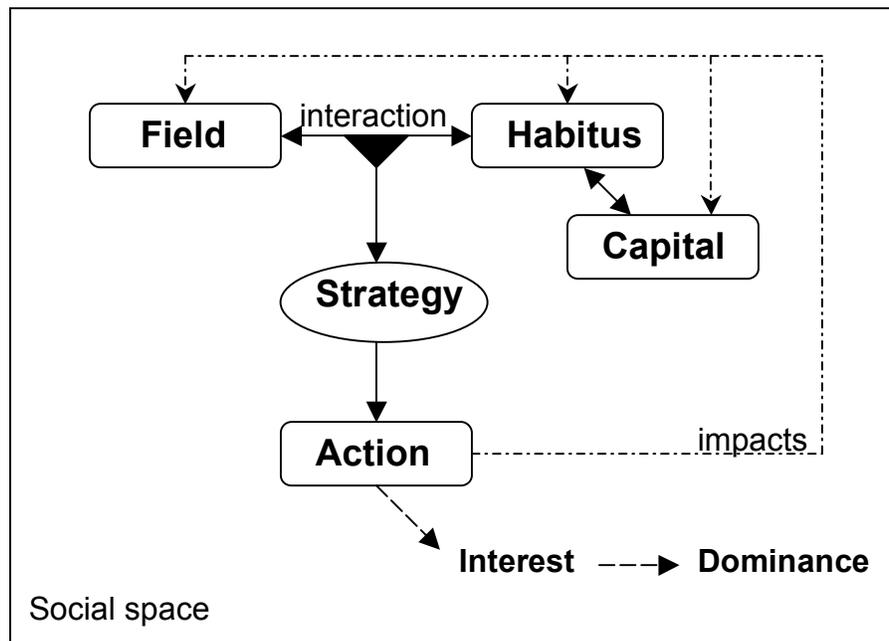


Figure 5.1: Bourdieu's cultural theory

A field is a structure of relationships between positions (Bourdieu and Wacquant, 1992). An individual or group is defined by the particular position it occupies in the field. This positional property cannot be assimilated to intrinsic properties (Swartz, 1997). A group distinguishes itself by way of its relationships with other individuals or groups in the field. There are numerous fields within a social space. Each field has a specific logic and principles. It also has a body of specialists who adjudicate practices, knowledge and products (Swingewood, 1991). As the social world is perceived to be relations between positions, there is a struggle for defining the

boundaries of a field. These struggles are seen to transform or conserve the field (Bourdieu, 1983). In essence, the fields are arenas for struggle for control over valued resources (Swartz, 1997).

Another important theoretical component of the cultural theory is habitus. It is a concept involving a set of subconscious fundamental dispositions that enable agents to interpret and act in a social world. Bourdieu (1971) explains habitus as “a system of lasting, transposable dispositions which, integrating past experiences, functions at every moment as a matrix of perceptions, appreciations, and actions and makes possible the achievement of infinitely diversified tasks, through analogical transfers of schemes permitting the solution of similarly shaped problems.” These dispositions are developed through early socialization process. Dispositions are acquired in social positions within the field and imply a subjective adjustment to that position (Mahar et al in Harker et al., 1990). The fundamental social conditions of existence are the ones internalized into dispositions. Such conditions are those that determine materially, socially, and culturally what the probable, possible, or impossible for a given social group (Swartz, 1997).

The habitus is affected by the changing conditions in ways that either reinforce or modify it (Bourdieu and Wacquant, 1992). There is an associated change in dispositions with a change in positions within fields. Such ongoing adaptation tends to find a compromise with the material conditions. That is, habitus is never fixed. The adaptation process is generally slow, unconscious, and tends to elaborate rather than alter fundamentally the primary dispositions (Swartz, 1997). The inherent bias lies in

the observation that the perception of objective conditions (of the material and social environment) is itself engendered and filtered through the habitus (Mahar et al. in Harker et al., 1990).

Capital is the third component in Bourdieu's cultural theory. It is the logic that orders struggles for position and legitimate authority in a field (Mahar et al. in Harker et al, 1990). Capital is a kind of "energy of social physics" (Swartz, 1997). Capital acts as a social relation within the system of exchange. It is applicable to all the goods that are perceived to be worthy of attaining in a particular social formation (Bourdieu 1977). The value given to capital is related to the social and cultural characteristics of the habitus (Bourdieu 1984). There are four types of capital – economic, social, cultural and symbolic. We can convert one form of capital into another under certain conditions.

Action is not a mechanical response to external determining structures. Rather, habitus shapes the responses to existing conditions by mediating the effects of external structures. That is, action is the product of class dispositions intersecting with the dynamics and structures of fields. The following is the equation as a summary of Bourdieu's cultural model , [(habitus) (capital)] + field = practice (Bourdieu, 1984). Action as strategy is to emphasize the interest-orientation of human conduct (Swartz, 1997). Interest is defined practically as whatever motivates or drives action toward consequences that matter (Bourdieu, 1987). These are embodied dispositions of actors that operate at a tacit, taken-for-granted level. Struggles are over the accumulation of any form of capital where strategy is used to maximize the profit.

5.3 Constructing the Field Map

Social space is a multi-dimensional space with an open set of relatively autonomous fields (Cheal, 2005). In the case of Information Technology Agency (ITA), there are two sets of fields that have an ongoing direct impact. One is the IT field, and the other is Government field. Here, we are concerned about both the fields as specific to the Commonwealth of Wonderland. In other words, although IT field and Government field have broader affiliations we are interested in field as specific to the Wonderland. The Government field of Wonderland has characteristics similar to that of any state government. However, it particularly differentiates itself as a commonwealth model of governance. The government field is comprised of the Executive, the Legislative and the Judiciary fields. Among these, the Executive field has specific implications for the ITA. Similarly, the IT field of Wonderland shares characteristics and concerns of IT in general, for example, shortage of trained personnel in security, it differentiates itself as being specific to the government organizations and in particular to the Wonderland. The IT field of Wonderland is comprised of further sub-fields. These sub-fields are, in fact, IT environment of different state government organizations such as the Department of Social Services and the Department of Motor Vehicles. Although sub-fields might share some similarities with the Wonderland IT field, these are specific to a particular organization's mode of operations.

In addition, different disciplines within IT can also be considered as fields that have influence on the ITA. Each discipline has logic and principles specific to itself, and body of specialists who propagate the practices and knowledge of that particular

discipline. The traditional disciplines of database and systems development form such fields. In addition, the IT Security field, the IT Auditing, the IT Project Management and the IT Governance are few other important fields for consideration. Fields underline the relational view of the social world (relations between positions), where boundaries of fields are themselves objects of struggle (Swartz, 1997). This is particularly true for emerging disciplines like the IT Security where there is no clear demarcation of the boundaries for the field. The IT Security depends upon good practices in all the disciplines that come together to form information systems. It encompasses the technical computer security (network), the IT auditing and the IT governance. However, it is still unclear as to what might be the definite boundaries of the IT security. We do have to keep in mind that the social space of the ITA is conglomeration of various fields. There are fields other than IT field and Government field that may be considered to have tertiary influence and as such, tertiary fields. The field of economics is considered to be the dominant one among all fields.

5.3.1 Understanding position of the security department

The impact of a position is based on its relation of dominance or subordination to other positions. These can be termed as a system of objective relation of power between social positions (Mahar et al. in Harker et al., 1990). These positions are subject to a certain distribution of unequal amount of different types of capital (Cheal, 2005). The possession of capital guarantees specific profits that are at stake in the field

(Bourdieu and Wacquant, 1992). These positions are also influenced by the present and potential situations.

Any change in a position would inadvertently involve redefining boundaries with respect to all positions. The struggle for position in fields is essentially a struggle for power between dominant and subordinate groups. The dominant groups have a degree of monopoly over defining and distribution of capital. “There is constant struggle between different classes and class fractions in society, who compete to impose the definition of social world that is best suited to their interest” (Bourdieu, 1991). In fact, fields can be considered to be the arenas of struggle for legitimation. Such a conception implies that fields involve resistance and dominance between positions (or groups).

The IT field of Wonderland is a structure of relationships between positions occupied by the government organizations. Each organization is subject to a certain distribution of different kinds of capital. One organization may be a big government organization whereas another might be a small citizen advocacy group. Both these types of organizations are endowed with different constitutions of capital. The former might be endowed with economic capital while the latter with a greater social and cultural capital. The position of IT Security department at the ITA may be considered as occupied by an institution. The IT security audit conducted by an auditing agency revealed poor security practices in state government organizations. As a result, a statewide endeavor was undertaken to secure the IT environment of the state government organizations. Legislation was passed that held heads of various

organizations as directly responsible for any security related adverse events. IT security was emphasized at all levels, although one may call this more of a window dressing. However, a central state initiative on IT security was embarked upon with the beginnings in the development of the IT security policy for the state. As a result, the IT Security department at ITA saw an increase in its strength of employees.

At the time of data collection, IT security is prominently visible among issues for top executives of the organization. The role of the department has shifted from providing direct services to that of governance. With recent shift, the role is seen more in terms of addressing compliance issues. This is also evident from the recent (time phase towards the end of data collection) merger of the security department with the auditing department. The new goal of the merged IT security department is to provide better IT security governance in the state. It would be practical to get all government organizations to have base IT security practices in place. The effectiveness of such efforts is expected to be evident in the next audit report evaluating security practices in the state.

The positions are also objectively defined by the structure of the distribution of species of power. For the IT security department, the legislation passed by the Wonderland empowered the CISO to ensure that the state security policy is complied by all government organizations. Needless to say, the symbolic power is very high and everyone tries to appease the CISO. This is true even in day-to-day practices of the department where the CISO might not even be present. During the committee meetings, members of the department would often conduct themselves in a certain manner that the

CISO prefers although it might not be a prudent approach to address a problem. All that members cared about was to make the CISO happy.

The symbolic power held by the security department is evident in the manner department can indirectly force other government organizations to spend required funds on security. The case in point is an extension of the deadline where organizations were to get compliant with the state security policy by July 1 of 2007. Many organizations did not have enough resources, either financial or human, to meet such a deadline. In fact, the ITA as part of an earlier consolidation had already appropriated most of the experienced IT employees of these organizations. Also, for many organizations there was not enough response time involved from the time of notification to the deadline for compliance. This was particularly the case for organizations with medium or small sized IT operations. The ITA extended its support to various organizations for getting compliant. However, there were many issues which would be discussed in the subsequent sections. It was made absolutely clear to organizations that they have to get compliant by the deadline no matter what. Also, there were only very few exceptions allowed since the compliance report was to be provided to the Governor. This led most of the agencies to divert their resources from other projects to getting compliant with the state security policy.

In the end, a day before the compliance deadline the CISO decided to extend the deadline for a period of another six months. From the CISO perspective, there were many organizations that would not be able to get compliant and as such, it was prudent to give blanket extension to everyone in the state. The extension on last day of

compliance did not go well with the majority of organizations. This move further infuriated many bigger organizations. These government organizations saw the deadline extension by the CISO as an exercise in wasting significant resources and efforts. The agencies argued that if the CISO knew that the deadline was to be extended why could not such a move be done earlier so that they could plan efficiently. Many organizations that did divert resources felt they could have done it properly or better if they knew about the extension in advance. Also, these folks felt they were made to look bad by security department with the extension. They felt their hard work went to naught, as they would not get any commendation from the higher-ups. Mostly, people were upset that they had to put other vital projects on backburner in order to divert resources to get compliant with the state security policy. Also, things would have been done more smoothly only if the CISO had trusted them with her plans. Many felt betrayed.

The ITA knew that the security policy was not up to mark and had issues with it. There was a general acknowledgement among the security department members that the policy had to be reviewed sometime in the future. The logic was to get something out of the door from the organizations to follow. The emphasis was to have basic security practices in place, although requiring improvement. Some members even joked that this approach would allow them to have some work to do in the next year. To sum it up, the whole exercise had wasted much needed resources. The very fact that majority of the organizations made compliance with the security policy as their priority despite vital projects suffering indicates the kind of symbolic power held by the CISO and the IT security department.

The security department enjoys a dominant position within the ITA and across the Wonderland. In fact, the CISO has direct access to the TIB, the Governor and the General Assembly of Wonderland. Fields are at all times defined by a system of objective relations of power between social positions which correspond to a system of objective relations between symbolic points (Mahar et al. in Harker et al., 1990). The Wonderland IT field is combination of all the IT fields of various government organizations. The social positions of these IT fields would include all government officials who may be able to influence the IT field in some form or fashion. These positions would include among others, the Governor, the Secretary of Technology, the CIO of ITA, and the CIO of various organizations.

Further, each government organization has few legislators that are sympathetic and support an organization's interests in the state. These politicians can put pressure on the current Governor directly or indirectly through various committees and commissions. Few of them also have influence on the TIB and other planning boards. In sum, the Legislators, the Governor, the Secretary of Technology, and the TIB members can put political pressure on the CIO of Wonderland to do things in certain fashion, which might not necessarily be conducive for the IT environment of the state. At the same time, reverse relationship also holds. If certain organization is not performing as expected, the CISO can report to the CIO or the Secretary of Technology who would hold that organization accountable. The Governor can also push the legislators to apply pressure on specific organization head for certain measures. In fact, the IT field of

Wonderland is defined by this system of objective relations of power between social positions in the field. These positions are in fact symbolic points for various institutions.

The positions in fields can to some extent be shaped by the habitus that actors bring with them. At the ITA, the Audit and IT Security were two different departments under previous CISO, Kevin Smith, who was in charge of security department only. After the exit of Kevin, the charge of security department was passed onto the Head of Audit department on a temporary basis. The position of CISO now was open to the influence of habitus of Jessica Anderson, the Head of Audit department. She had education credentials in accounting and vast experience in auditing. The positions once attained can interact with habitus to produce different postures, which have an independent effect on the economies of position taking within the field (Mahar et al. in Harker et al., 1990).

As the auditing background of Jessica interacted with the CISO position, a new posture emerged for Jessica that allowed her to perceive security as a compliance function. This posture was given a garb of educating users so that the users would know how to be compliant with the security policy and do right things. The interaction of habitus with the position led to more and more overlap between Auditing and Security functions. Eventually, the Auditing and Security departments were merged and the position of CISO evolved to become the Chief Information Security & Audit Officer (CISAO). This has led members of the department into uncharted waters where the function of security is closely associated with that of auditing. The customers of ITA

see the evolution of security into auditing role as more of a policing function that goes beyond mere governance.

Identifying position of the ITA security department in fields of interest

The struggle for position in fields opposes those who are able to exercise some degree of monopoly over the definition and distribution of capital and others who attempt to usurp the advantages (Swartz, 1997). Within the ITA, there is struggle for distribution of capital between the CEO, the TIB and the heads of various departments. Here, the CEO is part of the dominant class while heads of various departments are the subordinate class (table 5.1). The ITA has six major departments that have to constantly struggle amongst each other to attract maximum resources. These departments are: Outsourcing Management, IT Security, Customer Relationship, IT Solutions, Auditing, and General Administration.

Table 5.1: Position of ITA Security directorate in various fields

Field	Internal ITA field	IT Security field	IT field	Government field
Position				
Dominant	CEO, IT Solutions	ITA Security	Application development	Big government agencies
New entrant	Outsourcing Management	-	Security	ITA Security
Subordinate	ITA Security	Government agencies	-	Small government agencies

The Outsourcing Management department maintains the relationship with the Outsourcing Firm, which is the IT vendor for the state. This vendor has provided the state with much required funds that have been invested to develop the state-of-the-art data centers. As such, the Outsourcing Management claims to play an important role. The IT Solutions department develops all IT applications for internal use of the ITA. Therefore, they too have fair share of claim to importance.

As already mentioned, the state legislation mandates statewide compliance with the IT security policy within a stipulated time. This has attracted a lot of attention to the information security program developed by the security department. The development of security policy and the subsequent adherence is the responsibility of this department. The Customer Relationship department maintains the relationship between the ITA and various customers (government organizations). These organizations are sole source of revenues for the ITA and as such, customer satisfaction and feedback is of paramount importance. The Auditing, and the General Administration have generally been considered powerful in organizations. Needless to say there is constant jostling for resources between these departments as each lay claim to an important activity that would undermine the efficient functioning of the ITA as an entity. The merger of the Auditing department with the IT Security department may be seen as a step towards gaining significance in this struggle. Same individual heads both these departments and their merger is in fact consolidation of power to gain more capital from the dominant class.

At a broader level, there is an ongoing struggle for position between the Outsourcing Firm and the ITA, where the former is the dominant class and the latter may be considered as the subordinate class. The Outsourcing Firm has provided the state with much needed funds to be invested in data centers. Subsequently, it signed a contract with the ITA to provide IT services to the state. Now, the ITA finds it difficult to push the Outsourcing Firm to abide by the spirit of contract. The Outsourcing Firm is solely focused on providing services at cheapest cost possible. The aim is to provide minimum services possible while maximizing the profit. One cannot blame the Outsourcing Firm as it has to recover the funds provided to the state government as part of technology development. On the other hand, the state comprises of organizations with diverse needs and functioning. The contract that was written between the two organizations does not necessarily cover all the eventualities and necessities important to achieve a secure environment in the state. The contract is open for interpretation by either party. The Outsourcing Firm wants cost minimization that would be done by providing minimal services as necessary. On the other hand, the ITA has been arguing to abide by the spirit of the contract and not necessarily hold onto the exact wordings. Here, we see a daily struggle to gain resources from a dominant class.

There is a similar ongoing struggle between the ITA and various government organizations that are legally mandated to get IT services from the former. The law does not necessarily say so but there is only one IT service provider approved by the government, which is the ITA. Therefore, government organizations have to buy services from the ITA. As mentioned earlier, these organizations are the only source of

revenues for the ITA. There is suspicion among various organizations that the ITA aims to generate more revenues by over-selling their services. The ITA has not been able to shrug off this suspicion. They simply brush it aside citing historical reasons for such distrust rather than addressing these concerns. The government organizations as customers, which are the subordinate class in this relationship, have to constantly struggle with the ITA to procure necessary services and resources as required on time. They do have to guard against the predatory attitude of the ITA to generate more revenues. Some of these customers have full-time staff employed whose sole job function is to check against over-billing by the ITA on various transactions.

Fields denote arenas of production, circulation, and appropriation of goods, services, knowledge, or status, and the competitive positions held by actors in their struggle to accumulate and monopolize these different kinds of capital (Swartz, 1997). The fields are arenas of struggle for legitimation, for the right to monopolize the exercise of “symbolic violence” (Swartz, 1997). As such, the concept of field emphasizes the conflictual character of social life. These are sites of resistance as well as domination. There is a constant symbolic struggle between the different classes and class fractions in society, who compete to impose the definition of the social world that is best suited to their interests (Bourdieu, 1991).

5.3.2 Doxa

The general assumption among all groups is that the field of struggle is worth pursuing. That is, there is mutual understanding between groups on the stakes of

struggle. This deep structure of fields is referred to as doxa. It is essentially comprised of two opposing dimensions – orthodox and heterodox. The orthodox – heterodox opposition is a struggle for the “monopoly of cultural legitimacy and the right to withhold and confer this consecration in the name of fundamentally opposed principles: the personal authority called for by the creator and the institutional authority favored by the teacher (Bourdieu, 1971). Entry into a field requires the tacit acceptance of the rules of the game, meaning that specific forms of struggle are legitimated whereas others are excluded (Swartz, 1997).

The fields are characterized by competition. Individuals compete over different stakes, which could be converted to capital. All individuals try to increase the value of the species of capital that they possess and devalue the species of capital possessed by their opponents (Cheal, 2005). Few individuals would be more familiar with the rules of the game as compared to others. The analogy to game is used to describe the structure of relationship in the field. Such individuals would have greater capacity to manipulate rules because of their established capital appropriation such as qualification, occupational status or social status (O’Brien and O’Fathaigh, 2005).

Prior to creation of the ITA, the IT infrastructure was owned by various government organizations. These organizations had the freewill to spend IT budget as they saw necessary. At this point in time, these government agencies formed the dominant establishment in the Wonderland IT field. The state government entered the field as a subordinate challenger. The state government wanted to consolidate the IT infrastructure under a new entity called the ITA, which further outsourced the

infrastructure. The interference by the state government indicates that the field of IT in Wonderland is worth pursuing. The government had broader growth interests for the Wonderland in mind. The state got poor bond ratings as it was perceived to be risky essentially because of lack of proper disaster recovery mechanisms in place. The only way to avoid adverse rating was to develop a data center for backup and replace old IT equipment in the entire state.

In order to obtain such huge investment, the state developed Public – Private partnership which would allow to get the required money from industry. The private industry partner would develop two data backup facilities without any amount spent by the state. In essence, the private partner would be providing that state with soft loan without any interest. In order to staff these centers, the partner would also hire employees from the state human resource pool. Further, one of the backup facilities was to be located in the southwestern region of the Wonderland, which would bring much needed economic development to that part of the state. In return, the Outsourcing Firm has been made an exclusive IT outsourcing partner for the Wonderland. This was essentially a way to repay the loan amount. However, IT efficiency and reducing budget deficit were few of the reasons advocated in justification of the public-private partnership. Other players of the game, namely the ITA, the Outsourcing Firm and the government organizations also had specific interests to be gained.

The Outsourcing Firm's interest in pursuing the IT field in Wonderland was two fold. The partnership allowed the Outsourcing Firm to move into a lucrative market of providing IT services to the state governments. If successful, it would be able to make a

case for other states as well. Another interest is about the bottom line profit generated for the organization. The deal with Wonderland was lucrative for the Outsourcing Firm in its own right as one may argue that it already possesses the necessary expertise by virtue of working on big contracts and projects for the defense sector. For the ITA, the consolidation of the IT infrastructure would enhance its role in the state and make it more powerful for the benefit of its stakeholders. As customers, the government agencies seem to be at the receiving end in terms of shifting of infrastructure to the ITA although they still have to pay for these resources. However, these organizations have to rely upon IT for efficient delivery in order to provide the required services to citizens of the state. The efficient functioning of the customer organizations seems to be the reason for reliance upon the IT field.

The government organizations were holding onto the orthodox position that IT infrastructure and resources should be located or owned by respective agencies only. On the other hand, the state government was advocating for a heterodox position whereby all IT infrastructure and resources for the state would be consolidated. The ITA was to be a sole provider of IT services for Wonderland. The state government called upon the institutional authority of constitution and state legislation to propose the public-private partnership whereby the ITA outsourced the IT infrastructure. This move was strongly opposed by various state government organizations that cited personal authority to own the IT infrastructure and seek services from entity other than the ITA alone. In essence, the struggle between the state government and other organizations is the struggle for cultural legitimacy whereby each player wants to have the sole authority to proclaim

what constitutes as culturally legitimate. The legislation does not stipulate monopoly status to the ITA. That is, the state government agencies are not required to procure IT services from only the ITA. However, there is a tacit acceptance among the ITA, the agencies and the state government that organizations can only purchase IT services from the ITA. This is the only form of legitimate struggle. The action of procuring IT services from a new player (other than the ITA) is excluded as an invalid form.

Let us consider the appointment of CISOs at the ITA and their relative struggles. Prior to his appointment at the ITA, Kevin Smith had developed the security program for one of the government agencies in another state. The expectation at the ITA was to develop the IT security program at the enterprise level and move it away from an organization level. The position of CISO was to report directly to the CIO. At the very first day of joining the ITA, Kevin was told that he would not be directly reporting to the CIO but Steven Turner, the Director of Strategic Planning, which was later renamed the IT Solutions department. This can be seen as competition among key players who act as department heads within the ITA. Although Kevin as the head of IT security department was a key player, other department heads tried to undermine his power by influencing the decision and making him not report directly to the CIO. This resulted in problems with communication channels with top management. It was difficult for Kevin to understand what CIO's strategic direction was. As per Kevin,

The real impediment was communication channel. Although CIO wanted communication but it wasn't happening. I don't think things weren't properly communicated to CIO. Also, reverse route is important, that is, knowing what CIO's strategic direction is.

This resulted in further problems and his eventual exit from the organization. It is also interesting to note that Kevin did not fight but rather accepted the change in the reporting structure. This behavior may be attributed to a lack of awareness about the rules of the game since he was a new entrant. And also, Steven seems to have a greater capacity to manipulate the rules through his established capital appropriation with the ITA. The discussion about various types of capital would be undertaken in the subsequent section.

Essentially, the department heads were trying to show how important their group was so that their function would not be outsourced. The Strategic Planning group would become even stronger if the CISO in fact reported to head of the department. The underlying assumption is that people will usually work to increase the value of the species of capital that they possess (Cheal, 2005). One important consequence of the competitive logic of fields and their doxa is that they help create the conditions for “misrecognition” of power relations and thereby contribute to the maintenance of the social order (Swartz, 1997). In sharp contrast, Jessica Anderson, current CISO, took over the IT Security department as an additional duty. In her capacity as the head of auditing department, Jessica was reporting directly to the CIO and the TIB. She retained the reporting structure when she took over the duties of CISO. This can be seen as significant in power struggle where the CISO position has gained direct access to not only the CIO but the TIB as well. Eventually, to further devalue the position of the opponents Jessica was able to merge the security department with the auditing department. Needless to say, this move resulted in gain of significant stake and greater

appropriation of capital. Jessica's social status and prior work at the ITA helped her to wrench a significant stake away from the IT Solutions group.

The merger of security department with the audit department in fact creates a change within the ITA but has consequences beyond it as well. With merger, the role of security may be seen as evolving to that of governance and eventually to that of audit. This development in change of roles may be imitated by various government organizations that may perceive it to be the correct role as practiced by the ITA. In turn, organizations might decide to restructure their security and audit departments as well. Thus, individuals or groups employ strategies to effectively utilize their capital in order to differentiate themselves (from others) and attain a position of advantage. Such individual or collective strategies change and preserve the field itself (Swingewood, 1991). We will discuss strategies under section 5.4 'Strategizing for Action.'

5.3.3. Characteristics of fields

The fields are characterized by three properties: autonomy, mediation and homology. A brief description of these properties is provided in table 5.2.

Table 5.2: Characteristics of fields

Property	Explanation
Autonomy	Independence from external environment through internal mechanisms of development.
Mediation	External influences are retranslated into the internal logic of fields.
Homology	Reproduction of common patterns of hierarchy and conflict from one field to another.

Autonomy

Fields are autonomous from external environment to an extent. These are structured by their own internal mechanism of development. Each field has its own specific interests which might be different from external interests. Fields elicit assent to existing social arrangements and thereby contribute to their reproduction to the extent that they engage actors in field autonomy (Swartz, 1997). The political and economic power leads to the growth in autonomy of the field. That is, they gain in symbolic power, which gives the capacity to legitimate existing social arrangements (Bourdieu and Passeron, 1977).

The IT field of Wonderland has been influenced by the internal mechanisms of development. In the 70s and 80s, the IT infrastructure in the form of networks was centralized. As the requirements of organizations changed, the IT infrastructure was decentralized and owned by individual government organization. The role of ITA's predecessor changed to that of establishing policies and standards and developing strategic IT planning for the state. The development of IT field in the state indicates relative autonomy from external environment. The external interest for government might be to develop efficient solutions and provide effective services for the state. However, the professional interest of ITA's security department is to ensure that all organizations are compliant with the security policy. This would make certain that an audit does not indicate glaring security practices in the state. The actions of the security department do not indicate its concern about the potential problems created by the security practices for efficient development of an information system. In fact, various

stakeholders had repeatedly mentioned that security recommendations were being made with a complete disregard for the business requirements. One of the members considered “security as a necessary evil, where although it is necessary but more importantly it is evil.” This indicates significant deviation from external interests.

Let us take the case of the development and implementation of the security policy throughout the state. The ITA security department developed the security policy. All state government organizations were required by the legislation to get compliant with the state security policy by a certain deadline. In order to get compliant, customers would have to ensure that the Outsourcing Firm enforces the required technical measures. This indeed created some confusion with the customers. From customer point of view, the ITA is asking the organizations to ensure that the Outsourcing Firm, which is partner of the ITA, enforces certain technical measures. The security department members also developed the standards and guidelines that were provided to customers as a form of support. The ITA engaged the security officers from all government organizations through the forum of SAG meetings. The message of compliance with the security policy and new social arrangement was aggressively communicated. These officers would go back to their organizations and engage resources to begin the work to get compliant. In fact, many agencies diverted the resources from other business critical projects to meet the requirements of the security compliance. In essence, the ITA was engaging actors in the act of field autonomy.

The field of IT security was acknowledged in the state as various organizations diverted resources from critical projects. The customer organizations were to

unconditionally comply with the requirements of the security department in the form of the security policy so developed. Finally, the extension of security policy compliance deadline by the CISO was again an exercise to further legitimate the social arrangement. The manner in which the ITA security department indirectly forced various customer agencies to spend resources and money on getting compliant indicates increasing economic power of security department. The political power was wielded with the ease by which the CISO was able to extend the deadline provided by legislation on the last day of getting compliant. The political and economic power leads to the growth in autonomy of the field. Further, the security department pushed the argument that the Outsourcing Firm also needs to get compliant with the security policy. This met with a favorable response from the top management and power stakeholders in the state. The legislation and contract, which had been loosely drafted, was provided as documents supporting the argument. Such a measure was seen more as a mechanism of control over the Outsourcing Firm which had been dictating terms to the ITA. It allowed the CIO, Ian Martin, to use security policy compliance as a tool for leverage.

Mediation

External sources of influences are always mediated through the structure and dynamic of fields (Swartz, 1997). Such influences are retranslated into internal logic of fields. The federal government was not happy with the fact that the federal money provided to the Department of Social Work (DSW) would in fact be going to the ITA as the owner of IT infrastructure. As such, the federal government asked the DSW to stop

paying any invoices generated by the ITA. Such an action was considered by the ITA to be an external influence by the federal government. The problem was retranslated as one where federal government needs assurance that money for the DSW is actually being spent only on the organization. Subsequently, the ITA changed its pricing model where the DSW and other agencies were all charged under one pricing model, which was a flat rate per seat in that organization. For the ITA, such a move was premature since all organizations had not caught up with each other in terms of the IT infrastructure. There were still customer agencies that required significant investment in infrastructure. The new pricing model negatively impacts such small agencies that might not have required the budget.

Field homology

The autonomous fields are related to each other through structural and functional homologies. Homology refers to the isomorphic properties of the field such as position of dominance and subordination, strategies of exclusion and usurpation, and mechanisms of reproduction and change (Swartz, 1997). This means that individuals or groups in subordinate positions in a particular field would also find themselves in subordinate position in other fields. That is, the patterns of hierarchy and conflict are reproduced from one field to another field.

Based on the field analysis, the relation of supply and demand of the field of cultural production and the field of social classes, is mediated by field structures and processes (Swartz, 1997). The cultural products reflect the producer's position of

dominance or subordinate in a field struggle. These products are not reflection of consumer demands. “The logic of objective competition at the core of the field of cultural production leads each of the categories of producers to offer, without any conscious search for adjustment, products that are adjusted to the preferences of the consumers who occupy homologous positions within the field of power” (Bourdieu, 1984).

The security policy, standards and guidelines developed by the ITA security department are in fact its cultural products. Currently, the security department enjoys a dominant position within the ITA. However, members of this department had struggled to move it to a dominant position. The former CISO used to report to the Director of Strategic Planning. Now, the CISO has access to the CIO and the TIB as well. At the same time, the department is able to exert some influence on the Outsourcing Firm. The security policy, standard and guidelines reflect the dominant position of the struggle. Both these documents are comprised of the following domains: risk management, IT contingency planning, IT systems security, logical access control, data protection, facilities security, personnel security, threat management, and IT asset management. As one may infer, these domains are exhaustive and go beyond the technical aspects of an organization. If an organization needs to be compliant with this policy and standard it has to ensure that its designated the CISO indeed enjoys such dominant position so as to address all these aspects. Such a position would require access and influence across different departments within an organization.

Another important aspect to be noted is that the security policy and standard were not written by the ITA security department from consumer's point of view. This has been captured during interviews with various stakeholders within and beyond the ITA. The stakeholders generally complain that the policy have not been written with the business requirements in mind. Others complain that it just stands in isolation and is completely detached from the business reality. Such concerns further strengthen the argument that the cultural products reflect the respective positions of dominance or subordination of the producers rather than the demands of the consumers. The security policy and standard carry a hidden agenda then. Any government organization that would get successfully compliant with this security policy would in fact be able to do so by making the CISO a prominent position of influence across its organization.

The concept of field autonomy, mediation, and homology builds on the idea that legitimation of social class inequality is not the product of conscious intention but stems from a structural correspondence between different fields (Swartz, 1997). Actors unwittingly reproduce or change those class distinctions simply by pursuing their own strategies within the sets of constraints and opportunities available to them. Habitus is the real principle of the structure of the structural homologies or relations of transformation objectively established between fields (Bourdieu 1977). That is, it is the practical logic of habitus that makes the underlying connection across fields. However, since fields vary historically in the degree of autonomy from the economy, the polity, and class structure, Bourdieu claims that one cannot establish a universal classification system connecting the various fields (Swartz, 1997).

5.3.4 Summary

Field specifies power relation and hierarchy. These are the arenas of conflict and struggle over valued cultural resources. It is essential to identify the influence of various fields and map various positions so as to expose the opportunities and constraints offered by the situation. For the ITA, the two fields of prominence are IT field and government field. The convergence of these two fields generate opportunity and constraints for the social space defined by the ITA. There is mutual agreement among actors occupying the social space that IT security is worth pursuing in Wonderland. Towards this direction, legislation has been enacted that empowers the IT security department of ITA. It also provides legitimacy to the position of CISO in various organizations in order to achieve required degree of security. There is a tacit acceptance among various actors about the rules of the game in particular that only the IT security department at ITA is the legitimate provider of IT security services, as well as, authority on statewide security initiatives. Competition, as principal dynamic of the field, necessitates actors to be aware of the rules of the game. The significance of being aware of the game is evident in the manner that the current CISO was able to change the reporting structure so as to have direct interaction with the CIO.

The arrangement in the social space of Wonderland emerged whereby the ITA security department would take on the role of governance, the Outsourcing Firm would be responsible for technical aspects of security, and customer government agencies were to implement the recommended security controls. The arrangement also reflects

the struggle for cultural legitimacy whereby each player wants to have sole authority to proclaim what constitutes as culturally legitimate. In this struggle, the ITA security department has emerged to be a powerful player. One may attribute a part of gain in power to the legislation that empowers the security department to enforce the security policy. The power held by the security department is also evident in the manner that it forced customer agencies to divert funds and resources from vital projects to ensure security requirements. Further, the extension of compliance deadline on the last day was another powerful demonstration of dominance by the security department.

All this becomes even more interesting when we consider the mutual acknowledgement among members of the security department that the security policy is indeed flawed and need to be reviewed some time in future. The security policy in itself is a reflection of dominance of traditional disciplines of security like risk management, computer security, and emergency management. In order to successfully implement the policy, it would be essential for an organization to designate a CISO who enjoys a dominant position and have influence across the functional unit of the organization. Such situation might be considered as an opportunity for the security department while constraint for other departments.

Field as a competitive system of social relations functioning according to its own specific logic implies that the security department of ITA is indeed involved in the struggle for power with other players. Within the ITA, security has to compete with traditional dominant departments of IT discipline like the IT Solutions that are involved in developing applications. Then, there is struggle with other customer government

agencies to enforce establishment of ITA's view of security. Finally, the ITA security department also has to compete with the Outsourcing Firm for power where the latter enjoys the dominant role by virtue of being the financier to improve Wonderland's bond ratings. Further, by pushing the Outsourcing Firm to abide by the security policy, the ITA security department is in fact garnering political leverage for the CIO. Fields are considered to be the arenas of struggle for cultural resources. Such resources would include artifacts like security policy, and security standard. So why would players struggle or fight over these cultural resources. The answer is simple. Players fight for cultural resources as these would indirectly support in creating a position of dominance. That is, cultural resources obscure quest for power and dominance.

5.4 Understanding Habitus Peculiarities

We will explain the articulation of habitus in the case of ITA using the Standard Review Committee meetings convened during the months of February and March of 2007. The interactions and reactions of various actors or members of this committee would be used to explicate the characteristics of habitus. The nature of the meetings was to review security guidelines and also address the concerns received from various agencies so as to prepare the guideline for final publication release. The committee was comprised of Ashley Smith (Deputy CISO), Michael Smith (Security Manager), three external consultants, subject matter in-charge at security department, and representative of policy group from the IT Solutions department. The importance of the concept of habitus lies in the fact that it allows to explain how objective structures and subjective

perceptions impact human action. It is a way of explaining how social and cultural messages (both actual and symbolic) shape individuals' thoughts and actions (O'Brien & O'Fathaigh, 2005). The environment at the review meetings varies from collegial to serious and argumentative.

Let us consider the meeting to review the contingency planning guideline. During this meeting, the Lead Consultant, James Smith, was very upset with review comments made by one of the new external consultants. This member was relatively young individual specializing in information security from a local university. Overall, there was a lot of tension in the room as both members were arguing for their comments and observations. Basically, consultants were resisting each comment on the guideline. The concept of habitus fundamentally implies that past experience plays a significant role in dealing with present and future situations. Maybe, the resistant behavior on part of external consultants can be attributed to their frustration at having to address concerns from an academic. James did make statements on few occasions like "the comments are from an academic viewpoint," or "academic world is different than industry," and also "academics do not know what goes on in industry."

The habitus emphasizes the influence of historical, cultural and social contexts. In terms of historical context, James was frustrated with the number of times that the guideline had to go under revision. This concern was also expressed by Michael who mentioned that on average each guideline undergoes ten to twelve revisions. The influence of cultural context may be seen in the relative comfort of operation for the consultants in fast paced industry environment. They are still not used to working in the

government context. This was captured in one of the statements made by James stating that he was frustrated with how government institutions work and their lack of sense of urgency. The social context is brought about in the statements emphasizing the differences between university and industry setting. James understands the social fabric of the committee and decides to play this factor. A committee reviewing standard is expected to be more persuasive towards solutions that actually work in the industry rather than trying to implement or buy a concept that is yet to be tested (from academic world). As such, James employs the social distinctions to tilt the situation to his benefit. Habitus is the primary form of classification available to an actor.

An interesting observation is the manner in which the standard review committee members leave the meetings. The scheduling of these meetings is done ahead of time, generally couple of weeks in advance, and every member knows that they are required during the review process. However, members leave the meeting for reasons that seem to be trivial given the task of reviewing the standard. During the meeting to review the contingency planning guideline, one of the members with subject matter expertise (Sarrah Smith) had to leave the meeting to be at doctor's appointment. Another member, Ashley (Deputy CISO) had to leave the meeting early because she had to attend another meeting. The actions of all these members are bound by the objective social structures as internalized during early socialization experience. For both these members, the structure of commitments seems to be an overriding factor. The behavior to skip a meeting where task has not been accomplished seems to be rational so as to be able to make appearance for another meeting. These two members are not

concerned with getting a specific task complete; however, putting in presence at prior-committals seems to be the main objective. At the same time, one may also question the choice of the concerned actors in scheduling back-to-back meetings. Such behavior makes sense if we understand it through habitus. Bourdieu (1977) explains,

Habitus as an acquired system of generative schemes objectively adjusted to the particular conditions in which it is constituted, ... engenders all the thoughts, all the perceptions, and all the actions consistent with those conditions, and no others.

During this meeting, James ended up questioning the validity of continuing with rest of the review process as half the members of committee had left. The aim of the meeting was to complete the review of contingency planning and logical access control guidelines.

Let us consider another interesting observation that was made during the Standard Review Committee meetings. All members agree that there is a problem with the security policy and standard. However, they want to continue developing guidelines based on or in-sync with the flawed policy and standard. The emphasis is to get everything done for now and later revisit them and revise. The ITA security has to produce policy, standard, guidelines by a certain date so that the customer agencies are compliant by the deadline. The members argue that “let’s get the first version of everything out” and then we can go back and make structural changes to the security policy and standard. And, then guidelines can be tweaked for alignment. The question then becomes whether all this process is an eyewash? Should not the policy and standard be fixed first? Why waste resources on flawed documents?

The state government organizations in Wonderland have to implement these flawed documents and then, re-implement them again as and when changes are made to the security policy. This behavior on behalf of the committee members can be explained if we consider that such a behavior is actually based on the practical evaluation of the likelihood of success of such action. In the given situation with certain time constraints, the members believe that it is practically viable to develop guidelines based on the problematic policy and standard. The committee members provide the rationale that although problems exist with the current policy, there would be significant improvement or progress in moving from previous policy to the current one. The success has been reinterpreted as providing different agencies a minimal base for security rather than none at all. The problems with policy can be addressed in subsequent planned revision after July 2007. Habitus is based upon the "practical evaluation of the likelihood of the success of a given action in a given situation (which brings into play a whole body of wisdom, sayings, commonplaces, ethical percepts" (Bourdieu 1977).

Habitus would reproduce actions consistent with past experience in case of routine everyday situations. However, it innovates when confronted with new situations (Swingewood, 1991). The capacity to be inventive emerges from an experience and capital possessed (Bourdieu, 1985). This puts power and its legitimation at the heart of the functioning and structure of habitus. The committee members openly recall past experiences to enlighten the current problem. They then discuss this experience with other members present. During the meeting to review the Logical Access Control

guideline, the members brought up two situations specific to government organizations, let us call them the DEQ and the DES. In the case of DES, members discussed the case of resetting the password for a system. Members contemplated the situation where the DES sends the personal identification number (PIN) via regular mail rather than e-mail, and upon receiving PIN user logs on and selects a new secure password. The members are able to fall back on their experience in various organizations and develop statements that are (or would be) consistent with the ground realities and user habits in those agencies.

For the DEQ, as the organization is distributed across the state the system owners might not physically see other users. Also, they do not have help desk. In other cases, helpdesk is there but operational from eight to five. How does system owner access files to provide or authorize user access? Banking on the past experiences and outcome of various situations allows the members to effectively tackle the problem that they are facing. These problems pertain to the effectiveness of the guidelines. The actors are able to think about practical options that would work in a given situation. As in the case of the DEQ, members did consider the resources available to such an agency in terms of dispersed nature of organization and availability of help desk. This allows them to write an effective clause in the guideline that would withstand the tests of real world situations. This is in fact demonstration of the explanation by Swartz (1997) that the dispositions of habitus predispose actors to select forms of conduct that are the most likely to succeed in light of their resources and past experience.

There is a constant struggle between members during committee meetings about objectives of the guideline. The members regularly question as to what are they trying to capture. “Are we addressing concerns at business level or IT level? Whether we should educate users or simply stipulate what needs to be done?” Members are generally split in this regard. As per James, “Jessica wants user education.” Subsequently a member questions, “But where do we draw line? What constitutes (and how much) as educating users?” Jessica’s (CISO) emphasis on educating users can be explained in terms of her understanding of the situation with respect to the ITA and Wonderland. Jessica understands that the customer agencies have been stripped-off most of the experienced IT folks. These organizational members were reallocated to the ITA. For Jessica, the agencies have so far been in the dark related to security.

The current progress regarding accomplishing compliance with security policy, standard and guidelines has its own merit. However, Jessica seems to believe that if the focus of these documents were slightly shifted to also provide education to users on security aspects it would go a long way in making agencies aware of or understanding security issues and concerns. Herein lies another hidden understanding of rules of the game by the CISO. A user who has been made to appreciate the security concerns through education would also be more willing to muster necessary resources and open to make required changes so as to enhance the security posture of the organization. Later on, it would be relatively easier to build on that and improve the policy subsequently after compliance deadline. Agents act through ‘practical sense’ in which goals and ends are not determined solely through conscious, deliberate and rational

practice but flow from the socially constituted 'feel for the game' (Bourdieu & Wacquant, 1992). Habitus is what regulates interactions within a field in an observable, "objective" manner, affecting not only the individual but all those who interact with that individual (Lawley, 1994).

Habitus is most useful for explaining behavioral patterns in situations where normative rules are not explicit (Swartz, 1997). Habitus "maybe superseded under certain circumstances - certainly in situations of crisis which disrupt the immediate adjustment of habitus to field - by other principles, such as rational and conscious computation" (Bourdieu 1990). As a general rule, where material interest are considerable or the threat of violence eminent, it is less likely that prevailing powers leave the course of action up to the habitus and the more likely that action becomes highly formalized. Highly ritualized situations reduce (but do not eliminate) opportunities for strategy and innovation by habitus, whereas less ritualized ones enhance strategic opportunities (Swartz, 1997).

The Standard Review Committee meetings may be considered as situations that are less ritualized. The normative rules are not explicit as to how a certain comment or concern is considered as significant over the current clause in the guideline. Generally, the aim of the meeting is to generate consensus among the group. Even if there is only one member who has an issue or different perspective, that issue is heard, looked upon and deliberated. If the particular issue deserves even a bit of merit, the suggestions are included although the language would be changed. For the contingency planning guideline meeting, there are a lot of disagreements on each comment. In each case of

disagreement, James suggested language that catches the disagreeing member's sentiments and is at the same time agreeable to rest of the committee members. In short, there are lot of negotiations going on.

Habitus assumes a reflexive agent whose orientations to the social world is grounded in practical knowledge and between 'conditions of existence' and the variety of social practices the 'structuring activity' of human agents intervenes (Swingewood, 1991). The individual (Andrew Smith) who wrote the IT security threat management guideline has a technical background. During the meeting it was clear that Andrew does not have an overall understanding of organizational security. As per Andrew, intrusion detection, prevention and protection is 'the security.' For instance, Andrew considers recording log procedures as a strategy and not an activity. At one level, such a conception of IT security world can be good as we can cover various elements involved in intrusion detection which is based on the experience from the trenches (technical frontliners). However, a lack of overall understanding of information systems security can be disadvantageous as the guideline would fail to tie-in or fit-in with bigger security picture.

The emphasis of the threat management guideline seems to be on hacking (intrusion) although the members believe it could also be done by an internal employee. Further, the concerned guideline is written in a sophisticated manner rather than simply saying what is intended. It is as if the individual who wrote this guideline wants the subject to be given a revered status by their users. It is not a question of human agents adapting passively to a pre-given social world but of active creative agents open to

many possibilities, able to employ knowledge and skills in maintaining and advancing their position within fields (Swingewood, 1991). Thus, that person's knowledge has a genuine constitutive power and is not merely a reflection of the real world (Mahar et al. in Harker et al., 1990). Habitus is acquired in practice, in the activities of everyday life (Cheal, 2005). It preserves a sense of continuity working as non-conscious structuring principles governing the ways that the past plays an active role within the present (Swingewood, 1991). The dispositions of habitus represents master patterns of behavioral style that cuts across cognitive, normative and corporal dimensions of human action (Swartz, 1997).

Summary

For habitus, actors are adapting to external constraints and establishing distinction from other competing actors. Members of the ITA security department were acting as per the rules of the game and conforming to the expectations of the CISO. Even during the Standard Review Committee meetings, there was lot of negotiations among members of the department in terms of selecting a correct clause for the guidelines that would establish distinction. Few of the guidelines were themselves written in a manner to achieve a revered status in contrast to other areas of security. Habitus is based upon the likelihood of success of a given action in a particular situation. The pursuance of the security policy, although mutually acknowledged among the security department members as having flaws, is the result of a practical evaluation of the likelihood of its success in the environment of Wonderland. The emphasis of the security department to

establish a base security practice among all organizations was served by the security policy even though the policy needed to be reviewed in near future.

The IT Security Department at ITA was initially providing security services to the customer government agencies. The department was involved in providing services such as intrusion detection and prevention as well as incident reporting. With current CISO at the helm, the nature and role of the department evolved to that of governance function. Such direction may be attributed to the dispositions of management of the security department whom had significant past work experience in auditing discipline. In fact, the CISO was assigned the responsibility in addition to serving as head of the Audit department at ITA. The managing officers approached security from the position of auditing discipline, although it does not seem to be a conscious effort on their part. The management of security department saw the audit approach of compliance and governance as more likely to succeed given the opportunities and constraints of operating environment at Wonderland. Slowly and subtly, the security department evolved to play the role of governance rather than be a technical security help desk. The recent renaming of the position of Chief Information Security Officer as Chief Information Security and Audit Officer reflects the impact of dispositions of the management. The development of information assurance program in fact implies to be in compliance with the prescribed security policy and standard.

5.5 Appropriating Power Through Forms of Capital

Bourdieu treats capital as power relations founded on quantitative differences in amount of labor they embody. It is the study of how and under what conditions individuals and groups employ strategies of capital accumulating, investing, and converting various kinds of capital in order to maintain or enhance their positions in the social order that constitutes a central focus of Bourdieu's sociology (Swartz, 1997). Capital can be accumulated, and once accumulated it tends to persist (Cheal, 2005). The unifying feature of all the species of capital is that they require time and effort to accumulate. The essence of all capital is therefore accumulated labor time, which allows interconversion between different species of capital (Cheal, 2005). There are different forms of capital as discussed below (table 5.3).

Table 5.3: Types of capital

Type	Explanation
Economic	Material wealth in the form of money.
Social	A set of lasting social relations, networks and contacts.
Cultural	Culturally valued taste and consumption patterns.
Symbolic	Prestige, status, authority and legitimation.

5.5.1 Economic capital

Economic capital exists as material wealth in the form of money or things that can be converted into money (Cheal, 2005). Economic capital is the dominant type of capital in the sense that it is at the root of all the other types of capital (Bourdieu, 1986). All the other forms of capital, such as cultural capital, social capital and symbolic

capital, are in fact “transformed, disguised forms of economic capital” (Swartz, 1997). Every type of capital is reducible in the last analysis to economic capital (Cheal, 2005). Economic capital on its own, however, is not sufficient to buy ‘status’ or position – rather it relies on the interaction with other forms of capital (O’Brien & O’Fathaigh, 2005). As stated in chapter 4, the ITA has an annual budget of three hundred million dollars. The organization does not receive any budget allocation from the state government. The organization generates revenues by charging for the services rendered to the customer organizations. For IT, the consolidation efforts by the ITA are one of the biggest endeavors undertaken in terms of economic capital in the state.

5.5.2 Social capital

Social capital is the sum of the resources, actual or virtual, that accrue to an individual or a group by virtue of possessing a durable network of more or less institutionalized relationships of mutual acquaintance and recognition (Bourdieu and Wacquant, 1992). It exists as a set of lasting social relations, networks and contacts (O’Brien & O’Fathaigh, 2005). The volume of a person’s social capital depends on the number of people to whom she is connected, and on the amount of economic, cultural or symbolic capital possessed by each of those persons (Bourdieu, 1986). For the potential relationships between people to become actual relationships, however, they must be recognized and practiced through material and symbolic exchanges (Cheal, 2005). Only in this way will the relationships come to be experienced as necessary

relationships that involve mutual obligations as a result of subjective feelings such as gratitude, respect or friendship (Cheal, 2005).

The members of the IT security department at ITA indeed indulged in material and symbolic exchanges between security officers of various government agencies. The security department decided to develop guidelines that would help the agencies in implementing the security policy and standard. Agencies were to be compliant with the policy only. It was not mandatory for the agencies to use these guidelines. However, there were time and resource constraints on agencies in order to get compliant with security policy. The ITA security department considered the development of guidelines as a gesture of help and support for the agencies.

The security department also procured special resource packages on subjects like risk management from industry consortium or research organizations. These packages include white papers, practical approaches and document templates in order to perform a specific function. In addition, the subject matter experts were also invited to give talk at meetings, sessions on IT security were scheduled at government conferences, and security tips were broadcasted through weekly newsletters and emails. All these indeed constitute as material exchanges between the ITA security department and customer agencies. Further, the security department also extended its support and help to the security department of other agencies. The members were made available to address any concerns of agencies and also guide them as deemed necessary in their efforts to get compliant with the security policy. As the CISO, Jessica pushed the agenda of educating users at every level through various published documents and

forums. The gesture of extending the deadline for compliance may be seen as symbolic exchange between the two parties.

Investment in social capital acts as a kind of strategy which (unconsciously or otherwise) further serves as a mechanism to exchange other capitals (O'Brien & O'Fathaigh, 2005). In order to maintain the availability of other people's resources, it is necessary to maintain the relationships through a constant round of sociability (Cheal, 2005). This takes time and is also a drain on resources to meet the economic costs of sociability. In order to maintain the relationships, the ITA security department created a forum (SAG) to enable all the security officers in the state agencies to regularly socialize through monthly meetings. These meetings generally lasted for about three hours and had physical presence of over seventy officers. There were about fifteen officers who would participate over long distance communication.

At these meetings, the ITA and the Outsourcing Firm would provide an update on security endeavors across the state. These meetings were also used as a forum for educating users about security. As part of this effort, a subject matter expert would be invited to give a talk on a particular issue of concern. More importantly, the SAG meetings were seen more as a mechanism to generate social goodwill and support from agency security officers and also dissuade any voices of concern or dissent. The security department eventually created a Security Council that would serve as an advisory group for the department, comprising of security officers handpicked by the CISO from different government agencies. Again, this may be seen as an effort to gain social capital from certain groups in the state. Jessica decided to tap this social capital and use

it to generate a positive influence. The council would also serve as legitimating the actions of security department. Both the SAG and the Security Council indeed help the security department in generating necessary social capital essential for effective security posture of the state.

5.5.3 Cultural capital

Cultural capital is defined as culturally valued taste and consumption patterns (Bourdieu, 1986). It refers to the ensemble of cultivated dispositions that are internalized by the individual through socialization and that constitute schemes of appreciation and understanding (Swartz, 1997). Cultural capital is the knowledge and tastes that are transmitted within families and in schools, and that mark those who possess them as socially superior to those who do not (Cheal, 2005). It covers a wide variety of resources including such things as verbal facility, general cultural awareness, aesthetic preferences, information about the school system, and educational credentials (Swartz, 1997).

Cultural capital comes in three forms – embodied, objectified and institutionalized (Grenfell & James, 1998). Cultural capital exists in an embodied state as cultivated dispositions to be consumed only by apprehending their meaning. Such form of capital would include various schools of thought and philosophies from different disciplines. Jessica and Michael have significant background in auditing and approach information security as a compliance role. At the same time, Jessica is a firm believer in the school of thought that an educated user is the best form of defense. Such

dispositions are captured in different clauses in the security policy. Even in terms of IT security, both Robert Smith, the security architect of the state, and Jonathan Orion, the security architect for outsourcing management, have constant arguments on the language of certain items and their subsequent interpretation as they believe in different philosophies on how to develop good IT defense mechanisms. “Two security guys would have different answer on how best to develop architecture to security solution,” justifies Robert.

In an objectified form, cultural capital refers to objects that require specialized cultural abilities to use (Bourdieu, 1986a). Such objects would include security policy and standard documents, security guideline documents, and security manuals. The security audit manual may also be considered as an objectified form. Here, specialized cultural ability is required so as to be able to check for the presence of security controls. Technical systems to ensure security in an organization would also fall under this category of cultural capital. Intrusion detection systems are based upon different philosophy than intrusion prevention systems.

Finally, cultural capital in an institutionalized form refers to the educational credential system (Bourdieu, 1986a). Such capital includes the degrees and diplomas earned in a specific discipline from a university system or an institute of higher education. Here, the status of the institution also matters. The industry certifications and affiliations also fall under this form of capital. Each form serves as “instruments for the appropriation of symbolic wealth socially designated as worthy of being sought and

possessed” (Bourdieu, 1977). The currency of such capital forms has more to do with their symbolic appropriation than with their possession (O’Brien & O’Fathaigh, 2005).

Culture can become a power resource. This occurs when cultural markets emerge where investors exchange currencies, strive for profits, and, in the case of educational credentials in recent years, suffer from inflation (Swartz, 1997). Cultural capital is unstable in that its accumulation can be undermined by criticism and suspicion (Swartz, 1997). Knowledge and tastes are used by individuals to distinguish the members of one class from another class (markers of social class). Since knowledge and tastes are shaped by socialization and education, they are often related to family and class background. When they are passed from one generation to the next through socialization, they constitute cultural capital that serves to maintain class membership (Bourdieu and Passeron, 1977). The transmission of cultural capital is a hidden means for reproducing class position.

5.5.4 Symbolic capital

Symbolic capital is used to explain the ways in which capitals are perceived in the social structure such as status value attached to certain books, values, or places of learning (O’Brien & O’Fathaigh, 2005). It exists as prestige, status, authority and legitimation (Bourdieu, 1986). Symbolic capital is the ‘power of constructing reality’ (Bourdieu, 1991). It is the capacity to construct beliefs about the world and to make them seem real. Symbolic capital is the ability to define what is perceived to be the

reality of the other three forms of capital (economic, cultural, social) through the use of symbols (Cheal, 2005).

In the realm of information systems security, good security practices, security skills, and effective policy development generates appreciation and respect among the players in the field. Also, achieving specific degrees of IT security in an organization is greatly appreciated and looked up as model for other organizations to follow. The prestige of winning an award from a national body is another case of recognition. Such explication of perceptions leads to an increase in symbolic capital. The capital represents power over a field at a given moment in time (Bourdieu, 1991). The most powerful conversion to be made is to symbolic capital, for it is in this form that the different forms of capital are perceived and recognized as legitimate (Mahar et al. in Harker et al, 1990). It is through the acquisition of capital, and the use of symbolic capital to perpetrate symbolic violence, that classes ensure their own legitimacy and reproduction (Lawley, 1994). For Bourdieu, all individuals are capital holders and investors seeking profits (Swartz, 1997).

5.5.5 The field of power

The field of power functions as sort of meta-field that operates as an organizing principle of differentiation and struggle throughout all fields. The field of power is defined as the relations of force that will gain between the social positions which guarantee their occupants a quantum of social force, or of capital, such that they are

able to enter into the struggles over the monopoly of power, affect struggles over the definition of an extended form of power as crucial dimension (Swartz, 1997).

Bourdieu considers conflict to be the fundamental dynamics of all social life. At the heart of all social arrangements is the struggle for power. This struggle is carried out over symbolic as well as material resources. There are two major competing principles of social hierarchy that shape the struggle for power: the distribution of economic capital (wealth, income, and property), and the distribution of cultural capital (knowledge, culture and education credentials) (Bourdieu 1989). The distinctive preferences and practices of individuals and groups can be understood largely in terms of their distribution according to these two opposing types of capital (Swartz, 1997). The greater the difference in asset structure of these two types of capital, the more likely it is that individuals and groups will be opposed in their power struggle for domination.

In the case of Wonderland, the ITA is considerably high in cultural capital and low in economic capital (table 5.4). The security department at ITA employs members with considerable expertise. These members are also expected to hold CISSP certification as part of eligibility criteria. In terms of economic capital, the ITA has to depend upon the customer government agencies for revenues. Basically, agencies have to buy services from the ITA. The state government agencies can be categorized as either big or small in terms of size of operations. The big agencies have huge budget for operations and are also mature in terms of use of IT in daily business activities. These agencies may also be spread across the entire state. Needless to say, these big agencies are high on economic capital and cultural capital as well. Such agencies would also

have necessary expertise and background in the field of IT security. Although human resources were relocated to the ITA during restructuring, most of these big agencies have been able to retain in-house expertise. Few of them were able to do so by moving key personnel to positions of non-importance during restructuring.

Table 5.4: Constitution of capital for field of power

Organization	Cultural capital	Economic capital
ITA	High	Low
Big government Agencies	High	High
Small government Agencies	Low	Low

In contrast, small agencies in the state are considerably low on both economic as well as cultural capital. These agencies have a designated security officer who actually might be performing two to three different roles at the same time. In most cases, these officers do not possess any security background and experience as they were essentially hired to perform some other job function. However, the ITA is endowed with considerable higher cultural capital than rest of the customer agencies.

There is a constant struggle for power and domination in the information security field of the state. Both the ITA and big agencies have been trying to dominate the landscape. Small agencies are key players in this struggle since they have comparatively low quantity of total capital (economic and cultural). Now, the ITA and big agencies are on the opposite ends of axis where the former is low while the latter is high on economic capital respectively. In order to gain some advantage, Jessica decided

to gain support of smaller agencies in the struggle of power against big agencies. She strongly advocated the education of users as the underlying theme for every security endeavor be it security policy or guidelines. The emphasis was to provide help and support to smaller agencies as they did not have enough resources. The security department provided the rationale that it was important to first bring everyone upto a certain level and build a minimum base. However, the real intent may be seen as building the vital support for the ITA among government agencies.

Most of the big agencies were generally opposed to the idea of ITA and highly critical of any initiative launched by it. This was time and again expressed in the statements of various stakeholders at the ITA. The folks at ITA would consistently remark during the interviews that all agencies considered the ITA to be evil. “They hate us” was the general remark heard from Michael, security manager. The big agencies considered the ITA security members to not have any clue about what they were doing. The ITA organizational members consistently questioned the ability of security members to successfully perform even menial tasks as the use of office productivity tools. On the other hand, the smaller agencies greatly appreciated any help or support from the ITA as they had low cultural as well as economic capital. Such efforts were gladly accepted by capital deprived smaller agencies.

In terms of compliance, the situation in Wonderland was perceived to be such where big agencies were able to comply with the policy to a certain extent. In such an event, smaller agencies did not want to end up looking bad in front of the state legislators by failing to comply with the security policy. The big agencies wanted the

ITA security department to develop the security program that would benefit them and give good grades in terms of the security posture. However, it would not come as surprise that the members of security department wanted to call the shots in relation to security in the state, especially since big agencies were considered to be the major sources of revenue for the ITA.

5.6 Strategizing About Action

The struggle and strategy become tied together through the notion of the field, and are dependent upon knowledge, which has both active and materialist aspects (Mahar, et al. in Harker et al., 1990). “All knowledge of the social world, is an act of construction implementing schemes of thought and expression, and that between conditions of existence and practices or representations there intervenes the structuring activity of the agents, who, far from reacting mechanically to mechanical simulations, respond to the invitations or threats of a world whose meaning they have helped to produce” (Bourdieu 1984). Action is not a mechanical response to external determining structures. Habitus, traditions, customs, beliefs filter and shape individual and collective responses to the present and the future. They mediate the effects of external structures to produce action.

The idea of strategy as not conscious nor calculated nor it is mechanically determined, but is the intuitive product of knowing the rules of the game (Mahar, et al. in Harker et al., 1990). There is unwitting complicity of actors in pursuing their own vested interest. Agents then construct their social world and act to reproduce their

positions and to gain position in the social world (Mahar, et al. in Harker et al., 1990).

“The most profitable strategies are usually those produced, on the hither side of all calculation and in the illusion of the most “authentic” sincerity, by a habitus objectively fitted to the objective structures” (Bourdieu, 1977).

There are three types of field strategies (Swartz, 1997):

1. Conservation strategies tend to be pursued by those who hold dominant positions and enjoy seniority in the field. These sets of practices are designed to maintain position (Mahar, et al. in Harker et al., 1990).
2. Strategies of succession are attempts to gain access to dominant positions in a field and are generally pursued by the new entrants.
3. Strategies of subversion are pursued by those who expect to gain little from the dominant groups. These strategies take the form of more or less radical rupture with the dominant group by challenging its legitimacy to define the standards of the field (table 5.5).

Table 5.5: Types of strategy

Strategy type	Followed by	Aim
Conservation	Dominant group	Maintain position
Succession	New entrants	Gain access to dominant positions
Subversion	Dominated group	Radical rupture with dominant group

Bourdieu argues that behavior is strategic and not rule following or norm conforming. There is a certain interest, say x, which the dominant group is interested in. In order to attain x, the group follows practice y employing a particular strategy z.

There are quite a few practices and strategies available to choose from. However, the group chooses a specific strategy to achieve practice y. Such a choice can be explained as a function of interplay between field, habitus and capital. The emphasis is on the inter-relationship.

Let us analyze major actions undertaken by the ITA security department. We also have to keep in mind the relative position of the security department in the fields of its operations. As outlined in the field section, the ITA security department is under the influence of IT security field and government field in the state. Within the ITA, the security department is the dominated group, the IT Solutions is the dominant group, and the Outsourcing Management can be considered to be a new entrant in the competition for positions in the field. For IT security field, the security department at ITA enjoys the role of a dominant group. In this field, various government agencies may be considered as the dominated group. The government field in Wonderland has been dominated by big government agencies like the Department of Motor Vehicles and the Department of Social Services. As earlier stated, these agencies have sympathetic legislators who support different interests and concerns in the state. The security department, as part of the ITA, may be considered as new entrant in the competition for dominant position. The above discussion details position of the ITA security department during the empirical observation (data collection) phase. Now, let us consider major actions undertaken by security department and understand them in view of different strategy types.

Conservation strategies

One of the earlier action pursued by the IT security department at ITA was the formation of SAG as a forum for the meeting of information security officers from various government agencies in the state. This development may be seen as the pursuance of a conservation strategy. The dominant group pursues these strategies in order to maintain their position in the field. The SAG as an advisory group was formed to hear the concerns of various agencies and help them in some manner to implement the IT security policy. The basic aim was to help different agencies to achieve an effective information security in their respective organizations. However, upon closer scrutiny one may argue that the fundamental concern was for the ITA to make various agencies follow what it was preaching. The ITA security department was to be the dominant group and wanted other dominated agencies to buy-in their view of the world. Such a move would also thwart any attempt towards rebellion and channel voice of dissent in a controlled manner.

Lately, the SAG has evolved to be more of information sessions. Also, agencies started perceiving various initiatives of the ITA security department as a product of Jessica's (CISO) mandates or directives. These were seen more as whims of Jessica than as something conscious emerging out of real concerns. In other words, the dominated agencies started questioning the legitimacy and validity of the directives issued by the ITA security department. The growing concerns among agencies were seen as a threat to position of the ITA security department in the state. In order to undermine such threat and maintain its position in the field, the dominant ITA security

group decided to form a Security Council which would serve as an advisory role to Jessica. In her words,

I am interested in developing the synergy of councils and committees to help security initiatives. Currently, ITA is seen as dictating the terms or initiatives. With Council and Committee the program would be seen as a collective effort.

The council members would comment upon the security practices proposed by the IT Security department and also suggest other effective security practices for the Wonderland to be pursued. Such an action would be considered to be taken so as to maintain the dominant position. “It would be appropriate to say that I am driving them, security council, to do these initiatives,” says Jessica. Interestingly, the members of the council are selected by Jessica. This further supports the argument of forming the Security Council as a form of conservation strategy pursued by the ITA security department.

The emphasis of the ITA security department was to help smaller agencies in implementing the security policy. The argument provided for such an action was that of achieving a common base of security throughout the state. The security department further justified such an emphasis as small agencies lacked resources or expertise for appropriately implementing the security policy. This action may also be seen as an attempt to maintain the security department’s position. The ITA security department would be able to offset the influence of big agencies by gaining support of smaller agencies. The support shown by smaller agencies would put bigger agencies on defensive in terms of any actions undermining the legitimacy and dominant position of security department.

One of the latest instances of the conservation strategy was the extension of compliance deadline for the IT security policy. All agencies were to be compliant with the policy by a certain date. The security department projected their strictness about conformance with the deadline. Although agencies were facing difficulties nevertheless many took it seriously and diverted resources from key projects to meet the deadline. However, on the last day for compliance Jessica decided to extend the deadline. Agencies that worked hard to meet the deadline felt betrayed and cheated. As for many of them, time and resources have been wasted as they could have done an efficient job if they knew about the deadline extension earlier. Agencies suspected that Jessica knew about extending the deadline but purposefully did not let others know about it. On the other hand, the ITA security department argued that many agencies had requested for an extension of the deadline and there were others who were requesting for an exemption citing lack of resources. As these requests were being made close to the deadline, the CISO could only make such a decision now. This particular action of extending the deadline may be seen as demonstrating position of the group.

The extension on the last day signifies dominant position of the ITA security department in the field and also demonstrates the conservation strategy to maintain such dominant position. The ITA security department sent a strong signal to various groups by extending the deadline on the last day. As rumored by agencies, the deadline could have been extended earlier. But such a move would have been indicative of a weakening position where the ITA security department had to bend to the demand of agencies. However, by announcing the extension at the last minute the IT security

department gave demonstration of the dominant position enjoyed by them. At the same time, the IT security department was able to gain support of agencies that were unable to meet the requirements for compliance. Such an act would check any move on behalf of bigger agencies to undermine position of the ITA security department.

Succession strategies

Towards the last phase of empirical observation period, Jessica was able to change the CISO position at ITA and make it responsible for auditing as well. The new position was effectively renamed as Chief Information Security & Audit Officer and marked the merger of IT security and audit functions. This act of merger is consistent with the tenets of succession strategy. The succession strategy is followed by new entrants to gain access to dominant positions. As earlier stated, the IT security department at ITA is dominated within the organization by the IT Solutions department. Within the ITA, the Outsourcing Management department may be considered as a new entrant that gained prominence because of the crucial relationship between the ITA and the Outsourcing Firm.

The merger of IT security and audit functions would position the new department as a new entrant in the competition for the dominant position. Such an act is also reflective of the habitus of majority of the members of security department who possess significant audit background. These members perceive the role of IT security to be more of audit related. For them, it makes sense to merge the two functions as at one level their work may be seen in synergy with each other. In fact, Jessica (CISO), Ashley

(Deputy CISO) and Michael (Security Manager) consider themselves as auditors first. They joined the security department to gain experience in the latest IT concern – security, and be challenged. The consolidation of compliance and governance role under one roof would push the newly merged department in direct contention for the position of domination within the ITA.

At the beginning phase of the empirical study, it was observed that Jessica was anxiously meeting with the CIOs of big agencies in order to nurture their support, which was perceived to be essential in order for the information security program to succeed in the state. It was interesting to note that Jessica was meeting with big agencies while rest of the department members were visibly trying to help smaller agencies. In order to understand this observation, we have to consider the field of government at Wonderland. In this field, as stated earlier, the bigger government agencies enjoy the dominant positions while the ITA is considered to be a new entrant by virtue of legislation passed that indirectly confers such a title by consolidating all IT infrastructure of the state. The meeting of Jessica with the CIO's of big agencies may be seen as an attempt to gain access to the dominant position in the field. In essence, the CISO is trying to make agency heads realize that the ITA is indeed a new entrant. By seeking their support, Jessica is indicating that the security department at ITA is dependent upon big agencies and is not in a dominant position. However, the extension of support and abiding by the view of secure world by the agencies may be seen as a tacit acceptance of the ITA security department as a new entrant.

Once the ITA security department was accepted as a new entrant, it continued the push for access to dominant positions. The formation of Security Council may be considered as an action towards such an endeavor. By creating a Security Council and selectively appointing security officers of certain agencies, the ITA security department is indeed attempting to further fortify its quest for dominant position in the government field of Wonderland. The creation of a Security Council would further provide legitimacy to the directives of CISO. This would be further aided as the members of the council are selected by the CISO herself. The representation on council by certain big agencies would also strengthen the position of the security department against the influence of left out agencies. The creation of a Security Council interestingly aids the succession strategy adopted by the security department both within the ITA and the state.

Subversion strategies

Within the realm of ITA, the IT security department was in a dominated position. Kevin (former CISO) was not even reporting to Ian, the CIO of ITA. He was in fact reporting to Steven, the Head of IT Solutions department. As per Kevin,

The very first day I was told I would not be reporting to CIO but to Steven. From that point on, it was very much struggle.

This clearly reflected the dominant position enjoyed by the IT Solutions department.

The appointment of new CISO, Jessica, saw changes in the organizational structure of ITA. Upon taking charge of the office, Jessica started reporting directly to Ian. Such an action questions the legitimacy of reporting to Steven, the Head of IT Solutions. The

change in reporting structure is an example of subversion strategy pursued by the new CISO. The subversion strategy is followed by the dominated group for radical rupture with the dominant group by challenging its legitimacy. The newly appointed CISO was also the Head of the Audit function who reported directly to the TIB. By virtue of this position, she continued to report directly to the CIO in the capacity of the CISO also.

Another example of the pursuance of subversion strategy is the development of an information assurance program as an area for improvement in response to the audit report. In the IT field, the traditional view of security is one concerned with network security and incident security. The development of an information assurance program may be seen as making the definition of IT security a bit broader (or as extending the boundary of IT security). The interpretation of audit report by the security department as necessitating the need of information assurance program as an area for improvement is in fact questioning the legitimacy of the viewpoints of the dominant fields. These fields restricted the IT security to the domain of network communication and system administration only. As such, the development of an information assurance program is a radical rupture from the dominant traditional view.

5.7 Attaining Dominance Through Symbolic Value

In a given social space, there are different symbolic systems in operation at any particular time. Symbolic is defined as that which is material but is not recognized as being such (in a sense, a good accent, style) and which derives its efficacy not simply from its materiality but from this very misrecognition (Mahar et al. in Harker et al.,

1990). In the Commonwealth of Wonderland, there are different symbolic systems such as science, language, myth, discourse, art and religion. In the realm of information technology, the IT security as a discipline is conceptualized here as a dominant symbolic system. Of course, there are other disciplines as well operating in Wonderland IT arena struggling among different symbolic systems. However, the IT security currently seems to be dominant both in IT realm and the public space of Wonderland. There is growing concern among citizens about the security of their information and IT systems. In response, the state government has issued legislation that gives priority to IT security as a statewide initiative. Given such support from public and government, IT security has gained significant leverage within the ITA as well. On the basis of the state audit report, which gave bad marks to the state of security, the security department at ITA has moved itself to a position of heavyweight in the organization.

Symbolic systems are “codes” that channel deep structural meanings shared by all members of a culture (Swartz, 1997). IT security can be argued to be a cultural system which shares among its members a particular view of the world that is to make it more secure. The emphasis of the members of this culture is to provide assurance about the privacy of the information and security of the associated systems. All members have a firm belief that in order for the social world to be better it is essential to protect the information and systems from miscreants. Risk is prevalent in business world and it is necessary to mitigate these risks to an acceptable level. This can be done by proposing solutions that are based on the belief in either technical measures or behavioral aspects of the problem. However, there is a general agreement on what is considered to be right

or ethical practice. There is a constant struggle between black and white hats, where former are the miscreants or criminal hackers while the latter are considered to be good guys.

These systems make possible a consensus within the community as to the significance of the social world, as well as contributing to the reproduction of the social order (Mahar et al. in Harker et al., 1990). The social world provides the necessary monetary support for sustenance and also bestows upon the members a degree of responsibility and prestige. The members consider the profession to be worth pursuing. In the business world, there are executives that might not necessarily practice or pay attention to security. This belief provides the members with a moral responsibility to fight for good security practices. The symbolic systems as “structuring structures” are means for ordering and understanding the social world (Swartz, 1997). These may in fact be considered as classification systems.

The protection of information of the social world can be approached from the viewpoint of IT security, information system security, information security, information privacy, information assurance, auditing as policing role, and IT governance. The social order includes intellectuals (involving academic and industry researchers), technical practitioners, auditors, policy developers, and consultants. These are indeed the symbolic producers who create symbolic power. Then, there are the adversaries considered to be the black hat hackers, and rogue elements including mafia and criminals. There is a thriving underground black market to exchange the spoils of

computer crimes. A general understanding exists among the community about what counts as ethical or unethical in terms of security practice.

As a symbolic system, information systems security may be viewed as an art wherein the management of security requires proficiency in the art of security practice sometimes also referred to as soft security. Then, there is the science of IT security (hard security) that addresses problems associated with the technical system.

Information systems security has its own language, which captures the nuances of the discipline. There are acronyms and terms unique to information systems security.

Efforts have also been made to develop a dictionary of information systems security to explain the technical language.

All cultural systems are fundamentally human constructions that are historical, that stem from the activities and interests of particular groups, and that legitimate unequal power relations among groups (Bourdieu and Passeron, 1977). The symbolic systems perform three distinct functions of cognition, communication and political. These conceptual systems function simultaneously as instruments of communication and as instruments of knowledge (Bourdieu, 1971). The real political function that symbolic systems fulfill is their attempt to legitimate domination by the imposition of the correct and legitimate definition of the social world (Mahar et al. in Harker et al., 1990).

Robert, the security architect, narrated an incident where an ITA asset participated in denial of service attack against the University of Dreamland. As per Robert,

I have seen it at ITA in last two months. It happened at partnership location.

He commented on the incident as a reflection of poor user education and network management. Here, Robert was able to recognize the participation of an ITA asset in a denial of service attack as a security problem. IT security performs the cognitive function. It also embodies the knowledge that informs the security architect about the asset participation as a bad thing. The security architect is able to communicate the problem situation using the terminology specific to IT security. He also identifies possible areas of concern. IT security hence performs the function of communication.

Exposing another security professional to such an incident would evoke a similar response. That is, the use of an IT asset in a denial of service attack is not considered to be good. One may see symbolic systems as providing social integration at the level of communication while at the same time assisting in social differentiation in performing political function. By identifying poor user education and network management as the areas of concern, security architect is indeed advocating a specific definition of the world whereby network management is critical to avoid future participation in attacks. This is the attempt to legitimate domination. In this instance, IT security also serves the political function.

Let us consider another case as narrated by Justin Smith, the Incident Engineer.

People need to be told that they have to stop holding doors open for strangers. People do this out of courtesy for others. They try to be polite. However, they need to be made aware of the problems such behavior could trigger. In one case, I managed to get into some critical areas of an organization. It wouldn't have been difficult for me to install a key logger and capture login access information for various systems being used. If we focus on tools, it is consistently losing battle. The awareness training is the key.

In this particular case, Justin is able to recognize the problem as applicable to IT security. The problem is that people voluntarily let people inside a building so as to be courteous to each other. However, this poses a serious threat as it allows access to a person with malicious intent. The recognition of the problem also indicates that IT security serves as an instrument of knowledge. Justin demonstrates his knowledge, as he is able to understand the severity of threat. A key logger could be installed to capture login access information. A legitimate domination is intended when incident engineer suggests awareness training as the only possible solution. This is imposing a specific definition of the social world. Such attempt of establishing domination is further justified by support of a personal account.

The dominant symbolic systems provide integration for dominant groups, distinctions and hierarchies for ranking groups, and legitimation of social ranking by encouraging the dominated to accept the existing hierarchies of social distinction (Bourdieu, 1977). This dominant symbolic system utilizes the symbolic capital to gain symbolic power. The symbolic power exists when people voluntarily give up power over themselves to another, because they believe that the particular person has the power to do things (Cheal, 2005). Symbolic power is defined as “every power to exert symbolic violence, that is every power which manages to impose meanings and to impose them as legitimate by concealing the power relations which are the basis of its force, adds its own specifically symbolic force to those power relations” (Bourdieu and Passeron, 1977).

The legislation passed by the state can be considered as a form of symbolic power. It requires establishment of security practices and makes each agency head responsible for the protection of data and information of the state citizens. This may be considered to provide a guarantee to state a particular form of official nomination. The legislation places responsibility of protecting citizen information squarely on the shoulders of the agency head. This official nomination gives a recognized identity to the individuals holding the post. The agency head has to ensure that a particular government agency has indeed adopted required security practices. The legislation actually confers recognition on the agency head as responsible authority to institute best security practices.

In the struggle or conflict for the legitimate vision, a state named expert – the agency head or the information security officer - provides a point of view (such as in security policy) which confers universally recognized rights to others who hold certificate (of membership) and who act in the legitimate (expected) way. In a similar manner, the Executive Orders on security passed by the Governor may also be seen as a form of symbolic power. These Executive Orders pertain to the conferment of security responsibility on the Secretary of Technology who further has appointed the CIO of ITA as responsible. Such orders provide an official nomination for the conduct of and legitimizing a particular vision. The responsible officers indeed developed a vision to make Wonderland more secure, which is captured in the IT security policy. The policy further delegates rights to certain members of the organization who are expected to act in a manner congruent to effective security practices.

The symbolic power is used by dominant symbolic systems to perpetuate symbolic violence in the social space (figure 5.2). In symbolic violence, people recognize, or tacitly acknowledge, the legitimacy of the hierarchical relations of power in which they are embedded (Cheal, 2005). They therefore fail to see that the hierarchy is, in the last analysis, an arbitrary social construction which serves the interests of some groups more than others. The intent of the ITA and the state government to enforce the vision of secure information and information technology operations in the state is perpetuation of symbolic violence.

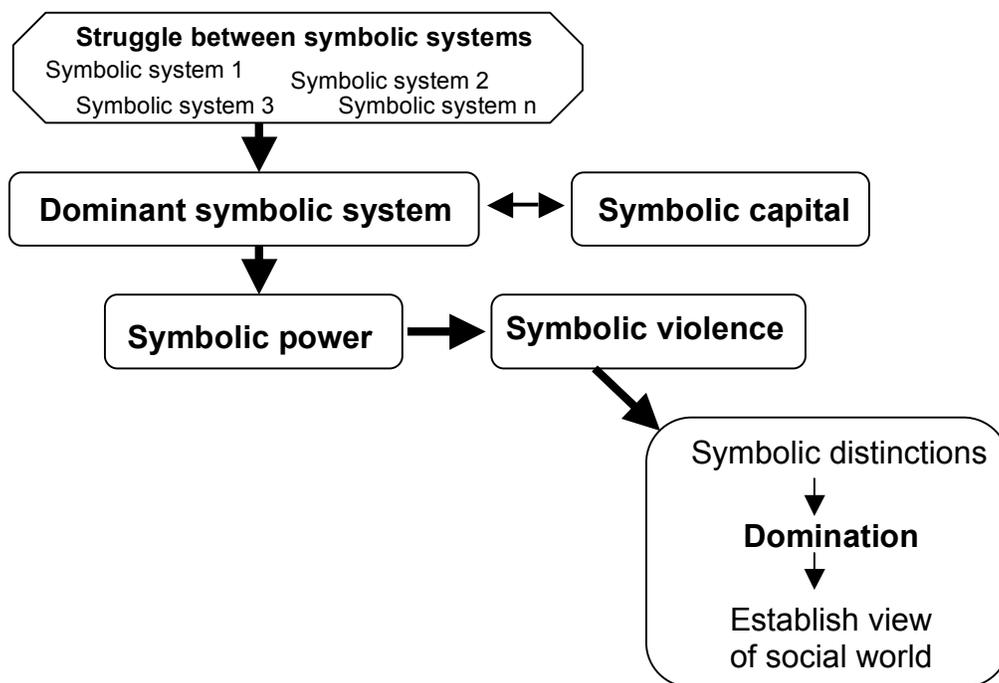


Figure 5.2: Dominance through symbolic value

The use of legislation and executive orders to force all the state government agencies to be compliant with the information security policy is an act of symbolic

violence. The ITA is using the symbolic power inherent in the position of CIO to enforce a certain vision about the social world. There might be agencies that do not agree with such a vision and might favor the vision of effectiveness over security. However, all agencies recognize and acknowledge the legitimacy of the of Wonderland and have to agree with such decrees as they all belong to the same social world. This is in fact domination of ITA (and IT security) over all executive government agencies.

The act of training the information security officers of various government agencies by the ITA security department is another instance of symbolic violence. In this case, the information security officers are inculcated in ITA's doctrine of IT security. The newly appointed information security officers are exposed to the view of IT security as mandated by the ITA to be legitimate. These officers are hence indoctrinated in a particular vision and would indeed mould their behavior to an expected performance. The aim is to make these officers take for granted the vision of ITA as legitimate and in fact propagate such vision in respective organizations. The majority of ISOs would fail to recognize that they can change such a social construction to their benefit. In essence, the symbolic violence is domination which is exercised upon social agents with their complicity because they misrecognize the conditions of their existence (Cheal, 2005).

The fundamental logic of symbolic processes and systems is one of establishing differences and distinctions in the form of binary oppositions (Swartz, 1997). In the realm of information systems security, there are a few paired oppositions with the fundamental one being whether a particular system has been hacked or is secure. The

dominant systems use symbolic violence to differentiate and legitimate inegalitarian and hierarchical arrangements among individuals and groups. The fundamental bipolarity is the dominant and dominated paired opposition (Swartz, 1997). “All agents in a given social formation share a set of basic perceptual schemes, which receive the beginnings of objectification in the pairs of antagonistic adjectives commonly used to classify and qualify persons or objects in the most varied areas of practice” (Bourdieu, 1984).

The distinctions established in information systems security are evident in the binary oppositions of being compliant - non-compliant with a policy or standard; ethical - unethical behavior; white hat - black hat hackers; good - bad security practice; effective - ineffective security controls; hacked - reliable system; hard - soft security approach; responsible - malicious code; restricted - open access; and confidential - exposed information. The binary logic of symbolic distinction determines our mode of apprehending the social world; it predisposes us to organize the social world according to the same logic of polarity and thus to produce social as well as cognitive distinctions (Swartz, 1997). Few other symbolic distinctions that are found in information systems security practice involve hacker - cracker; public - private keys; protected - unprotected information; open - closed port; available - unavailable system; trusted - risky environment; master - secondary level; cooperative - uncooperative behavior; encryption - decryption, to name a few.

The struggles between symbolic systems is to impose a view of the social world which defines the social space within which people construct their lives, and carry on the symbolic conflicts of everyday life and the use of symbolic violence of the dominant

over the dominated, that is education, relationships in the workplace, social organizations, even in conceptions of good taste and beauty. Symbolic struggles over the perception of the social world can take two different forms (Mahar et al. in Harker et al., 1990). On the objective side, one can act through the representations (both individual and collective) in order to demonstrate and valorise particular views of reality. On the subjective side, one can act through using strategies of self-presentation, or by trying to change categories of perception and appreciation of the social work.

The security group at ITA has embarked upon the strategy of projecting themselves as the policy group or as the planners. The security department is to develop the policy, standards and guidelines for the state, while individual agencies are expected to implement these. However, the ITA security department would provide guidance to agencies as the need arose. This is the subjective side of the symbolic struggle. On the objective side, the security group at ITA has been trying to attain the identity of governance or policing for Wonderland as applicable to IT security. Towards the end of data collection period, the management of security department released both their Security Incident Engineers. This action on behalf of the security department may also be seen as a way of shedding the identity of security technicians and moving towards the image of governance role.

The intent of the security department is to project the department as the governance group for Wonderland. This is evident in the emphasis of the department on policy development process only, while implementation process has been given the neglect and made the responsibility of individual customer agencies. The security

department aims to direct all the agencies as to what needs to be done in terms of information security. However, agencies often complain about lack of support and guidance from the security department for implementing the security policy developed by the very same department. Such concerns have been regularly raised during the SAG meetings.

At the ITA, there is also a struggle between security and systems development as symbolic systems. The security policy has strict clauses that would have an impact on the systems development process. In fact, these clauses direct the systems development group, which is the IT Solutions at ITA, to implement specific controls so as to ensure that the systems development process has taken security into considerations. Brian Turner, the IT Solutions manager, remarked that such controls are very restrictive and often do not make any business sense.

Tell me what the risk and tradeoffs are. I will take business decision depending upon the acceptable level of risk. Do not tell me that certain security control has to be implemented.

Such controls only take one viewpoint - that of security. It can be seen that there is an ongoing clash between the two symbolic systems of security and systems development to impose a particular view of the world.

For security, the aim is to make the world more secure, whereas systems development believes in making the world more efficient with the development of information systems. Similar struggles are also going on among other symbolic systems. For instance, the auditing discipline believes in a world where everyone is compliant with a given law, policy or standard. Such a worldview would again not sit well with the notions of systems development discipline. The aim is to make possible a

science of the dialectical relations between the objective structures and the structured dispositions within which those structures are actualized and which tend to reproduce them (Swartz, 1997). Social structures become internalized into the cognitive structures of individuals and groups who then unwittingly reproduce the social order by classifying the social world with the same categories with which it classifies them.

To surmise, there are struggles between different symbolic systems in a given social space. The dominant symbolic system uses the symbolic power gained by increasing symbolic capital to perpetuate symbolic violence. The aim of symbolic violence is to create symbolic distinctions in the social world so as to establish domination of the dominant symbolic system. The fundamental gain in such legitimation is to impose a certain view of the social world which would also define the social space.

5.8 Discussion

The aim of the IT security department at ITA is to establish a particular view of the social world, which is to make it more secure in terms of information and technology. That is, the overarching goal is to establish dominance of IT security in a social space defined by the boundaries of Wonderland. Bourdieu's cultural analysis helps us to understand the critical role culture plays in this quest for power. The dynamics of power intersect with all aspects of cultural life. Culture obscures the quest for dominance and provides tools for social distinctions. The ITA security department was indeed pursuing quest for class power. The security program developed for the

government agencies in the state not only addressed the prevalent IT security threats but was designed to gain power for the respective security departments as well. All the actions undertaken by the security department were consistently geared to move it towards the position of dominance. The IT security department wanted to have a dominant role within the ITA. Similar was the case for the government field in Wonderland where it was considered a new entrant. Culture may be considered as practices following common master patterns over cognitive, corporeal and attitudinal aspects of action.

Practices are the result of dialectical relationship between fields and habitus. Field specifies power relation and hierarchy. The convergence of the IT field and the government field generates opportunity and constraints for the social space defined by the ITA. There is a mutual agreement among actors occupying the social space that IT security is worth pursuing in Wonderland. Towards this direction, legislation has been enacted that empowers the ITA security department to enforce the security policy across the state. There is also tacit acceptance among various players about the rules of the game. The arrangement in the social space has emerged whereby the ITA security department took on the role of governance, the Outsourcing Firm became responsible for technical aspects of security, and the customer government agencies were to implement the recommended security controls.

The above-mentioned arrangement also reflects the struggle for cultural legitimacy whereby each player wants to have sole authority to proclaim what constitutes as culturally legitimate. In this struggle, the ITA security department has

emerged to be a powerful player. This becomes interesting when we consider the acknowledgement among members of the security department that the security policy is indeed flawed and need to be reviewed some time in future. As such, one may infer that security policy was actually used as an instrument to further the political interests of the security department. Fields are considered to be the arenas of struggle for cultural resources, which would include artifacts such as the security policy, the security standard, and the security program. The question then arises as to why players would struggle or fight over such resources. Players fight for cultural resources as these would indirectly support in creating a position of dominance for them. That is, the cultural resources obscure quest for power and dominance.

For habitus, actors are adapting to external constraints and establish distinction from other competing actors. It is based upon the likelihood of success of a given action in a particular situation. The pursuance of security policy, although mutually acknowledged among the ITA security department as having flaws, is the result of a practical evaluation of the likelihood of its success in the environment of Wonderland. The emphasis of the security department as to establish a base security practice among all organizations was served by the security policy even though the policy needed to be reviewed in near future. With the current CISO at helm, the nature and role of the IT security department at ITA has also evolved to that of governance function. Such direction may be attributed to the dispositions of the management of security department whom had significant experience in auditing discipline. These managing officers saw the audit approach of pursuing compliance and governance as more likely

to succeed given the constraints of the operating environment at Wonderland. Slowly and subtly, the security department evolved to play the role of governance rather than be a technical security help desk.

The fields and habits interact in a dialectical relationship to generate practices where capital also plays a significant part. The opportunities and constraints of the situation interact with the expectations of success, and abundance of specific capital influences generated practice. At the ITA security department, the development of an information assurance program, the formation of a security council, and an extension of the compliance deadline may be considered as major actions undertaken recently. The development of an information assurance program may be seen as an interaction between opportunity offered by the current state of knowledge in IT security field and audit dispositions of the security department management. The understanding that the security group is strong on cultural, social and symbolic capital helped in legitimizing such initiatives.

Actors are strategists where strategy is the tacit calculation of interest and pursuit of distinction. All behavior is strategic and not norm conforming or rule following. The actors follow conservation, succession or subversion strategy at any given moment to achieve a certain interest through practice. The security group at ITA is interested in establishing a particular view of the world. They want to achieve dominance in the social space through projecting their image as that of governance group. The security group was restructured by the CISO to put emphasis on establishing an information assurance component in the department. The department previously was structured

around the major components of the security policy that were advocated by a committee external to the department. The tacit rule is to act as per the direction provided by the committee. In the government field, it is a norm not to fight against the system or change things. One may pursue additional objectives but not on the expense of changing the current view. However, the CISO was not interested in following rules or conforming by the norms but was rather strategizing to achieve her interest.

As the security group was in a dominated position within the ITA, the CISO pursued a subversion strategy of developing an information assurance program. Information assurance challenges the traditional view of IT security and has broader implications involving formal aspects of security as well. Further, information assurance in essence implies compliance with a security policy and standard. Such a view is also consistent with the nature of auditing discipline. This would also be germane to the later evolution of the CISO position to that of CISA. This new position as a result of pursuance of successive strategy led to an increased power and dominance within the ITA. The development of a Security Council as part of conservation strategy pursued by the security group within IT security field would indeed support future legitimizing of components of the security program as deemed necessary in pursuit of dominance. The initiative as directive from the Security Council would be seen as collective effort rather than as an act of domination.

The cultural resources and practices attain symbolic value and aim to establish unequal social relations. This in fact is emphasizing underlying social classification. The legislation enacted by Wonderland to establish security practices may be

considered as a form of symbolic power. The legislation and security policy as a cultural resource legitimizes a particular vision of the social world as propagated by the ITA security department. The compliance with the security policy by customer agencies does in fact amount to perpetuating symbolic violence. The tacit acceptance of the legitimacy of the hierarchical relations of power is also evident in the practice of exposing newly appointed ISOs to ITA's doctrine of IT security. Such practice helps in establishing social distinctions in the form of binary oppositions like secure and non-secure, and compliant and non-compliant. These oppositions do point to a fundamental distinction of dominant and dominated where the ITA security department is the dominant player while customer agencies are dominated who are expected to accept the view of the world as recommended by the ITA security. The establishment of social distinctions is indeed synonymous of achieving power. The principle of power is the struggle between a group with cultural capital and another group with economic capital. Power formally acknowledges the dominance of a certain view of the social world. In this case, it is the dominance of the view of the world as a secure one rather than an effective world.

The cultural analysis indicates that practices lead to cultural continuity rather than change as the social structures are reproduced through the inter-relationship between field and habitus. The dialectical relation between habitus and field suggests occurrence of three kinds of situations in terms of the opportunities and constraints of the field in comparison to the situation in which the dispositions of habitus were first internalized (Swartz, 1997). In case where the opportunities and constraints of the situation are

similar to when dispositions were internalized, habitus will produce practices that correspond to existing structures. When field changes gradually, habitus tends to adapt as it addresses present situation in terms of past experiences. The practices so generated lead to gradual modification of structures. In situations where there are considerable discrepancies, rapid transformation can take place. The quick change in opportunity structures of the field would frustrate the expectations of habitus. This would result in possible social crisis amounting to resignation or revolt.

For Bourdieu, the last situation brings about change albeit an extreme one. This is the only form of real change as the change associated with the other two situations are more of cultural continuity rather than cultural change. The former two situations in fact reproduces the existing social structures. The source of change may be attributed to the lack of perfect fit between habitus and field. In order to introduce an initiative effectively, we should focus on structural lag or imperfect synchronization rather than be concerned with structural contradictions that would generate change.

In the extant literature, an organizational culture is generally perceived as an end in itself. That is, it has been proposed that one would be able to achieve certain goals like secure organization, or excellence in quality if there was indeed a culture sympathetic towards such an aim. This line of argument is fine so long as we are sensitive to understand that the true colors of culture are in fact those of power. The main tenet of Bourdieu's cultural theory is that culture is a tool for distinction and gaining dominance. It has emerged to be a softer form of coercion. One may very well agree to the view that culture is the glue that binds everyone in an organization.

However, the real objective of culture is to establish social distinction and hierarchy, and dominance of powerful class in a social space. This is why it can be the most effective tool for the management as a dominant class in an organization. The management also needs to understand the importance of education as establishing social classification through cultural distinctions. Formal education may impart socialization in a particular cultural tradition, reproduce social class relations and perform legitimating function (Bourdieu & Passeron, 1977). Bourdieu's cultural analysis implies that the practices actually signify cultural continuity. When we talk about cultural change we should rather consider continuity, as we do not want to cutoff the linkage with rich historical context. Change may amount to social crisis which is generally difficult to manage.

5.9 Conclusion

This chapter has described information systems security initiative from a cultural perspective. Such an approach was argued to be helpful in formulating the content of the initiative with respect to its context. The analysis in this chapter has evidently shown the effectiveness of Bourdieu's cultural theory to explain the intricate relationship between content, context and process in an organizational setting. A security initiative would be successfully instituted in an organization if it indeed were harmonious with the cultural continuity of an organization rather than significantly changing the existing opportunity and constraint structures leading to frustrating the

expectations of actors. Organizational culture may be used as a tool for coercion to establish dominance that would allow propagating a secure view of the social world.

CHAPTER 6

Implementation of Strategic Information Systems Security Initiatives at Department of Transportation

6.1 Introduction

The case study described in this chapter concerns the institutionalization of information systems security program at the Department of Transportation (DOT). At the time of study, the management of DOT was involved with a new statewide legislative requirement to get compliant with the state information systems security policy. The ongoing information systems security related changes were the prime motivator for this study. In this chapter, the structuration theory (Giddens, 1984) is used to understand the efforts to institute the security program at DOT. Once the content of the security program such as the security objectives, policy, and standard is decided, it becomes generally clear as to what needs to be done to achieve the specified objectives. These objectives might entail embarking on a particular set of actions. The correct implementation of such actions necessitates appropriate understanding of organizational environment or context. For implementation purposes, the relationship between process and context of an organization needs to be properly studied. The structuration theory is

employed in this chapter to particularly analyze the link between process and context dimensions as well as the content and process linkage.

This chapter is divided into six sections. The next section describes Giddens' structuration theory and its main theoretical components. This is followed by structural analysis of information systems security initiatives at DOT. Section 6.4 analyzes the empirical data from the perspective of Giddens theoretical perspective on modernity. Section 6.5 identifies the key findings for discussion. Finally, section 6.6 concludes the interpretation of information systems security initiative in an organization from a structural perspective.

6.2 Giddens' Structuration Theory

The structuration theory provides an interesting view on the relationship between agency and structure. The emphasis of the theory is on the interaction of human actors and structure resulting in a duality of structure.

By the duality of structure I mean that social structures are both constituted by human agency, and yet at the same time are the very medium of this constitution (Giddens, 1976).

Blaikie (1993) explains the social structures as perceived by Giddens to be both the conditions and consequences of social interaction. These structures are the rules and resources social actors draw on as they engage each other in interaction. These are not patterns of relationships. For Giddens, the social structures are not external to the social actor but rather they exist in memory traces and are embodied in social practices.

The structuration theory is specifically employed here because of its explicit focus on the social practices and their transformations. For Giddens (1984), the domain of study as per structuration theory

...is neither the experience of the individual actor, nor the existence of any form of societal totality, but social practices ordered across space and time (pp. 2).

The structuration theory has been extremely used in the management field to study organizational change. Walsham (1993) was among the early information system researchers to recognize the usefulness of structuration theory as a means to understand the link between context and process. Researchers have successfully demonstrated the use of this theory as a subtle and intricate approach to the interpretation of social systems. As stated previously, the main purpose of this research is to understand how to institute strategic information system security initiatives in an organization. The structuration theory lends itself to study this research problem. Another factor to employ structuration theory as a theoretical basis has been the philosophical position assumed by the theory. This theory embodies the argument to go beyond agent or structure (micro or macro) position and provides an alternative solution through the interaction between the two. As a result, the agents are considered as capable and knowledgeable and not merely “cultural dopes...of stunning mediocrity” (Giddens, 1979). In addition, the structure is to be viewed as rules and resources which are implemented in interaction. It should be used in a manner similar to “as an individual draws on the rules of grammar” and not “as a kind of framework, like girders of a building or the skeleton of a body” (Held and Thompson, 1989).

For the purposes of this chapter, we would employ the structuration theory in the tradition of its use by Walsham (1993) to conceptualize the link between context and process. The explanation of the analytical dimensions of duality of structure is based primarily on Walsham's (1993) explication of the theory. Walsham (1993) provides a schematic chart (figure 6.1) to understand the analytical dimensions of structuration theory. In this model, the social structure interacts with human actions through three modalities of interpretative scheme, facility and norm. The social structure is perceived to be comprised of three dimensions of signification, domination and legitimation. These dimensions interact with the three dimensions of human interaction namely communication, power and sanction. Interpretative schemes are stocks of knowledge that are used during communication and drawn upon by human agents to make sense of actions. This results in production (and reproduction) of meaning structures, which are essentially structures of signification. The structures of domination are impacted as agents employ power in interaction through various facilities available such as ability to allocate resources. Finally, "human agents sanction their actions by drawing on norms or standards of morality, and thus maintain or modify social structures of legitimation" (Walsham, 1993).

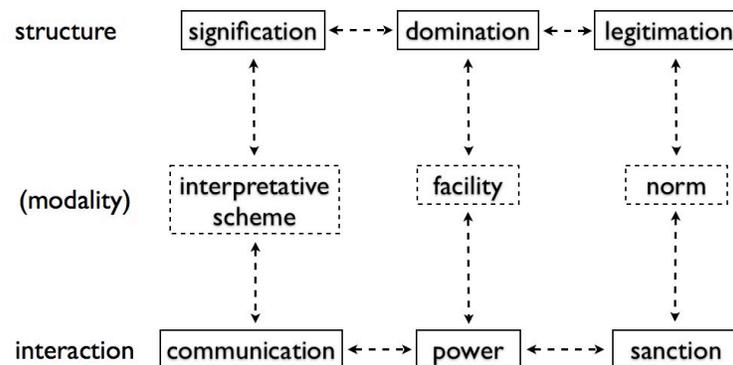


Figure 6.1: Structuration theory by Giddens (reproduced from Walsham 1993)

The structuration theory also lays emphasis on social interaction as occurring in time and space. The social actors are able to reflexively monitor their interaction through discursive consciousness. They rationalize their actions and provide reasons for any action. Blaikie (1993) explains that such accounts may depend upon “practical consciousness (which may be tacit and cannot be readily articulated); and, unconscious motivation (repressed semiotic impulses of which the social actor is usually not aware.” All action is nevertheless constrained by unacknowledged conditions and unintended consequences. Thus, every act that has the potential to reproduce any ordered form of social life carries with it the seeds of change (Giddens, 1993).

For empirical analysis, the modalities of interpretative schemes, facilities, and norms provide a means to link action and structure. Information systems may be seen as involved in these modalities that link social context and process in organizations.

Walsham (1993) argues that computer-based information systems embody interpretative schemes, provide co-ordination and control facilities, and encapsulate norms. Further, these systems are able to impact the existing structures as they are drawn on in the social processes.

6.3 Shaping Information Systems Security Initiatives at the Department of Transportation

The Department of Transportation (DOT) is a government agency falling under the Executive branch of the state. A new legislation was enacted in 2003 to address the growing concerns about information security in the state. The Governor and the state legislature sanctioned the statewide information security initiative. The legitimation of this initiative was sought by appealing to the norm of secure environment for the state citizens. This new legislation required all government agencies in the state to ensure good information security practices. The norms of viability and effectiveness were also utilized for the operations of government organizations. The aim was to achieve shared structures of signification. A secure environment would be conducive for effective operations for the state constituents involving citizens, businesses, and government agencies. The enacted legislation also held the Head of each agency as responsible for any adverse security incident in their respective organizations. The emphasis was to signify the concern for information protection by way of having consistent secure procedures and practices in various state agencies. A common interpretative scheme

was sought to be obtained through centralized or uniform security program with minimum set of objectives as benchmark for all organizations.

6.3.1 Designing information systems security initiative

In this case, the emphasis on information systems security emerged from the state legislature and office of the Governor. We can see the use of power to act arising from the structures of domination inherent in governing the state, and in lawmaker position. The state government wants to have a centralized security program for the entire state to enable change in structures of domination and exert closer control on compliance from various state agencies. However, the government agencies have protested against a blanket program by appealing to the norms of desirable levels of autonomy. The government believes that power inherent in the legislation would force the state agencies to use their facility of resource allocation to commit significant resources for the achievement of good security practices. At the minimum, the threat of legal statute and auditing would push the agencies to use the facility of coordination and control to get compliant with the state security policy. Subsequent legislation required all agencies to be in compliance with the state security policy by a specific deadline. As a result, the information security operations came under greater scrutiny by the DOT management.

Restructuring the organization for effective information systems security

The information security program has traditionally been responsibility of the Division of Operations Security (DOS), which had evolved from the Emergency Management Department (EMD). The DOS was essentially responsible for the security of the DOT operations. This responsibility included protection of critical infrastructures like bridges and tunnels, protecting building blueprints and related material, and protecting information (both financial and other) pertaining to construction projects. The DOS was established out of three and a half million dollars assigned by the Secretary of Transportation to the DOT as an emergency fund when a suspicious pipe was found beneath one of the bridges. “When there is an incident, there is fear and dollars get allocated,” says ex-CSO Karl Davis “That’s a big problem – educating people.”

By July 2006, the DOT was required to be in compliance with the revised IT security policy of the state within a year. To meet the compliance deadline, the top management at DOT used their position of authority to make information security the responsibility of the CIO Adam Martin and appointed him the CISO as well. Subsequently, information security operations were formally moved from the DOS over to the Division of Information Technology (DIT). Further, management used the facility of control to reduce the cyber security aspects of the organization from information security to IT security. As the CIO, Adam employed his authoritative position’s facility of appointment to place IT security operations under the supervision of the IT Governance manager, Camila Green. As Kevin Simmons (Deputy CISO) recalls,

The governance group was formed to maintain quality control and red tape compliance. When Adam got the responsibility, I guess he could have made a separate manager to deal with security but he didn't do it. Camila told Adam that only place for security to go in Adam's organization was to put it in Governance, as he was trying to change organization.

Camila depended on the norm of efficiency to justify her suggestion to Adam as "things were not happening fast enough." For her, the best organizational structure in terms of information systems security would be "to have one separate organization where security has all components like physical, COOP, BIA under one umbrella." Given the limited time frame, Adam then decided to approach the security policy compliance as another project. This reflects his belief in the norm of effectiveness in sanctioning such an approach. Utilizing his facility of allocating personnel, Adam brought in one of his trusted manager, Kevin, to achieve the security policy compliance by the required deadline. "I took security as just another project," says Kevin. Essentially, from July 2006 onwards, the security initiatives at DOT were shaped by the CIO as a practical response to the constraints of external context in the form of state legislation. It is also interesting to observe that the CIO did not appoint Alex Simmons, the former IT security manager at DOS, as in charge of the new information systems security initiative. Needless to say, Alex was bit bitter with this development. Kevin justifies the CIO's move as "Adam deals with known quantity only and he didn't know Alex."

The restructuring of IT security operations from the DOS to the DIT evoked mixed reactions among the stakeholders at DOT. Alex considered the restructuring as a complete violation of best practices. As per Alex,

The CIO decided to move IT Security to the IT division as bridge security is actually with the bridges division. Fundamentally this may be true but you don't put any pavement with security.

Kevin contends that such sentiments can be attributed to the fact that the CISO position was created at DOS with Alex. However, pointing to norms of effectiveness, Kevin thinks that not much progress was made in terms of IT security with Alex at the helm. As a result, the top management decided to use their authority to appoint Adam as the new CISO. “We were floundering before, now we are focused and disciplined,” says Adam. However, Alex did not agree with the view and argues that several conflicts of interest emerged between the IT department and security function even in terms of allocation of resources. He contends, “Resources were taken away from IT security and given to IT.”

Similar concerns were also aired by ex-CSO, Karl Davis who asserts that organizational structure was changed to move IT security operations to the DIT as it was not able to control security earlier. “It was a political decision,” says Karl. The DIT wanted to be in control of the security program and policies being developed at DOT. This was because the security policy would have direct implications on the way of developing applications and systems. Essentially, the DIT feared that a security policy that would be adverse to their interest could impact the interpretative schemes of IT development. In effect, it would have a direct impact on the day-to-day operations of the department. “IT thought they can’t abide by policies that we hadn’t written,” contends Karl. So, the DIT used the structures of domination and legitimation to move

IT security under their control. The department also used structures of signification to make a case for the DIT as the rightful home for IT security.

From the CIO's perspective, the change in organizational structure made sense for the DOT. As Adam observed,

Did we have competent people? Did we have IT people? What about technical structures? ... In the DOT, because of people, resources, dependency on IT, security wasn't working.

We can see Adam depending upon the norms of effectiveness to justify the current organizational structure. Although agreeing with the effectiveness of such structure, Kevin did see potential conflict of interest by having IT security under governance. The IT auditor for DOT, Craig Ernst, was more assertive in talking about such concerns. For Craig,

Security folks try to influence developers. Push comes to shove who will win, of course developers.

This again highlights the threat of change in interpretative schemes of IT development at DIT. Lamenting upon political aspects of the decisions, Karl attributes the disassembling of the DOS to the feud between the Director of the department and the CEO of the agency. As per Karl, "swords are drawn all the time" at DOT. The then Director of DOS had a military background and built a robust security program division through his power to use facilities of coordination and control. The Director was amply supported by the Secretary of Transportation because of personal reasons. This did not go well with the CEO of the agency. Subsequently, the CEO used his influence of

power to hire a new director to run the department. “DOT brought the new director to break it up,” asserts Karl. Such statement exhibits the acknowledgment of underlying structures of domination as emanating from the CEO position.

Generally agreeing with such assertions, Alex reformulated the problem as a case of different personalities. “The earlier Security Chief had a strong personality, but the next Chief did not,” said Alex. The issue of personalities was indeed a concern grasped by Kevin as well, who went to the extent of emphasizing the dependence of strategic initiatives upon the personalities of people in charge. For Kevin,

Why people get or join a position? What brought them here - the whole background is important. The strong or weak personalities of people play a lot important.

It seems that security best serves the needs of the organization if it is structured as an independent department reporting directly to the CEO. Some might consider such structuring to be essentially serving a governance function. In sum, we may say that the events unfolding at DOT, influenced by the circumstances of both internal and external context led to restructuring of the organization. The aftermath of an internal power feud between the Director of DOS and the CEO and the necessity to abide by the norm of compliance in the case of state security policy created a favorable situation for the DIT to get IT security operations under its control. The top management was indeed looking favorably upon disassembling the DOS, while the DIT wanted to control the IT security policy development to maintain the significance structures of IT development.

And, the limited time frame for the security policy compliance gave both the interested parties a perfect justification for such an excursion.

Developing organizational information systems security program

Around September 2006, top management of the DOT decided to approach IT security as a project. The aim was to get compliant with the state security policy by the prescribed deadline. Based on the belief in norm of effectiveness, it was decided to simply adopt the state security policy and standard so as to share same structures of signification as inherent in the state policy. The CISO Adam Martin justified such a move by stating, “Either create one or adopt from somewhere.” The DOT had an existing security manual of about thirty pages based upon an old security policy of 2001. For internal use purposes, the CISO decided to reconfigure the security manual as per the organizational requirements of the DOT but aligned it with the state security policy and standard. That is, the manual was given the same look and feel as the state IT security policy in terms of the structure, thus avoiding any confusion. This indicates an emphasis on proper communication to obtain same interpretative scheme.

The security group reviewed the policy and standard along with the industry best practices. “We embellished the state program to fit DOT organization,” states Adam. Here, the norm of appropriateness and effectiveness is used to sanction the actions of the security group. The security manual was developed with same chapters as those of the state security policy. The task of the group was to develop each chapter of the security manual as per the DOT requirements. The facility of control was employed by

the group to decide not to go beyond the state standard. As Kevin recalls, “if standard says a, b, c we won’t go and say do a, b, c, d, e, f.” The emphasis was to simply document the security program at DOT as a manual. Such an approach would allow effective communication of the program as sharing same structures of signification as are imbibed in state security policy.

The IT security group comprising of seven members were assigned individual areas of responsibility to develop the manual. The facility of coordination was utilized to review the developing document as a team. The reviewed document was then passed onto various committees for approval. It went through an organizational review process so as to abide by the norm of participation and obedience to evoke structures of legitimation and domination. The security group established and documented procedures for those areas that were covered by the manual. The group utilized the facility of coordination to conduct risk assessment even though it was system owners’ responsibility. For Kevin, “we are doing it to train them and help them in doing it.” The intent here seems to be in advocating the correct interpretation of a program component so as to share similar structures of signification. In case of disaster recovery, the group had to start from scratch and document all procedures as they found that these were not even documented properly. In addition, these procedures were also not being tested adequately. The aim was to put the building blocks in place for various components. The group decided to reconduct the BIA as business needs keep on changing even though it was not up for review. The data classification was done as per the new criteria and all systems were reassessed for sensitivity. This exhibition of the norm of help is

indeed designed to legitimize the move of IT security group to the DIT. Additionally, the DIT also wants to utilize the norm of progress to justify the organizational restructuring.

The problem faced by Kevin was to determine how far to go in terms of assisting others in their job functions. “The challenge is in getting people to be responsible for what was part of their jobs,” states Kevin. There were certain instances where things were not done as necessary in direct neglect of norms of responsibility. For instance, the awareness and training program was not functional. The security group approached such issues as per the established procedures. They would follow the procedure and get the specific component to be operational. Once it was operating they would hand it over to appropriate employees to take charge. Such an approach was in fact pushed down by the CISO. As Kevin recalls, “Adam would say that lets get it done and then we will sort out the responsibility mess.” The facility of coordination was used by the CISO to promote the above approach of getting things done. The aim was to signify for others that things were getting done in terms of security. The norm of responsibility was respected. In doing so, the actions of IT security group were further legitimized and also communicated a good image of the DIT. The security manual was completely developed by January 2007. It detailed the security program in seventy-five pages.

Although the security group seems to have adopted the inherent security objectives of the state security policy, the members themselves were trying to formalize their perceptions on the objective and the role of IT security. Some, like Wade Green in

the IT governance group, even discern between information security and IT security emphasizing that “T does not matter.” However, the group members seem to follow and articulate the views of Adam who considers the role of security to be about governance and technical issues. The articulation of similar views by the group members indicates their preference to abide by the views of authority. In doing so, these members are in fact acknowledging the structures of domination at work. Adam believes that IT security need to address what the policy is and how to implement it with technology.

For Adam,

It’s a holistic issue. We can’t say it belongs to left or right. It is about day-to-day activities coming from system engineering issues, and is not an audit issue.

Slightly deviating from such views, Camila Green, the manager of the governance group, considers the role of IT security to be addressing more of procedures and process than technical or audit aspects. She fundamentally agrees with the CISO on the role of security being more governance rather than that of audit. This again indicates alignment with the authority views. For Camila,

It is more procedures and process than technical or audit. Implement it as process that’s more important. I don’t like the concept of audit as security. It gives negative connotations.

She asserts that security should actually portray “someone watching not after but proactive.” Adam prides himself in the approach taken to develop the security program whereby the focus has been on the practical issues of security and using technology to make security transparent. Such approach exemplifies his belief in the norm of effectiveness to evoke the structure of legitimation. “I do not want to create security so that it is burdensome work for employees,” states Adam. The emphasis has been on

getting organizational members abide by the security requirements minimally. The logic pursued by the CISO can be summed up as the need to keep all members aware of security, to force them to make it absolutely necessary, however, do not make it bureaucratic.

6.3.2 Instituting information systems security initiatives

The information systems security program at DOT was approached in two phases. Once the security program was developed, the program need to be instituted across the organization. The efforts of security group to institutionalize information systems security program at DOT are described and analyzed in this section.

Evoking obedience through management leadership

The IT security program manual developed by the security group was presented to the CEO who approved it. The CEO sent out a memorandum addressed to various division heads of the DOT emphasizing his commitment to enforce the security program manual so as to meet the state security policy compliance deadline. Here, the CEO used the power inherent in his position through a memorandum, which represents a facility of control, to evoke structures of domination exhibited in his commitment to enforce a specific manual. He also used the norm of compliance with a state law to legitimize his action. The CEO also informed the divisions of his decision to adopt the state security policy and standard while creating the IT security program that reflected the adoption of the state policy. The memo essentially directed the divisional heads to

understand, acknowledge and agree to enforce and practice the tenets of the IT security program. The memo was used as a communication between the CEO and the divisional heads to achieve a shared structure of signification. This directive essentially implies the use of power on behalf of the CEO to force agreement from divisional heads using the facility of control and coordination to enforce the security program. Further, the memorandum invoked the inherent structures of domination to hold each division head as responsible for implementing the security program in their respective divisions and be also subject to routine audits. Kevin considered the memo to be a forceful one indicating that there would be no exceptions.

The strong leadership was a desired factor for the security group to achieve compliance with the security program manual. The leadership as constitutive of power held by an agent was seen necessary to sanction abidance with the security objectives as being communicated through the security manual. As Camila asserts, “That gives you stick to get people to do it.” Another group member, Alex emphasized the role of management as the force behind the rules. Such leadership would entail a lot less resistance to security efforts across the organization. The underlying assumption is that actors perceive management as the rightful party to tap structures of domination to enforce a particular action. Kevin also voiced similar sentiments.

The CEO had written a forceful memo. There was no question for anyone whether to do it or not. Most were aware they had to do it so they didn't fight us.

Remindful of the strong traits for the CISO as well, Brenda Simmons (security analyst at the department) considers it to be critical “that he is out there and bold so that everyone can see.” For Kevin, the security program was sold as a top-down approach

with directives coming from the state, in the form of security policy, to the DOT. Such an approach clearly laid down the authority. The communication of security objectives through the security policy and the program manual was to provide a common interpretative scheme so as to achieve the shared structures of signification across the organization. The use of state security policy for the DOT was morally sanctioned through the norm of compliance with law that drew upon the structures of legitimation possessed by the law forming body of the land. The relationship between the state government and other state organizations assumes the domination of former over latter respectively. This relationship along with the corporate position of the CEO was used effectively through the facility of control to enforce IT security program upon all divisions at DOT.

Creating user awareness by employing training as a compliance stick

The next step was to create an awareness of the security program among all employees at DOT. Adam recalls, “We developed security manuals and officially promulgated it so that every executive is aware of it.” The aim was to communicate the security policy across the organization so as to provide a common interpretative scheme for all employees. Such proliferation would also help in achieving a shared structure of signification, which in this case would be to achieve a secure mode of operations. Such a task created another challenge for the security group members since they had to deal with the realities of a functionally and geographically distributed organization. “It would be unrealistic for me to talk to everyone as folks are located remotely,” says

Brenda. To overcome such challenges, the security group resorted to conducting workshops for the officers of responsibility from each division. The scheduling of workshops illustrates the use of facility of coordination by the security group members and the workshops itself are being employed as a medium of communication. It is interesting to note that the security group decided to concentrate on only powerful agents. This selective behavior could be understood if we look at these officers of responsibility as the ones who would be able to evoke the structures of domination. These officers would be able to use power inherent in their positions to implement the IT security program in their respective domains. During the period from February to July 2007, the group conducted four awareness workshops although not on a regular interval.

The security group created a website and developed a prominent position on the organizational portal for incident reporting, awareness training, the security program manual, the security policy, and cyber tips. In other words, the group used the available resources and the facility of coordination to develop a website which served as a medium of communication for different components of the security program. As Kevin notes,

Lot of awareness went into it. For instance, in case of data protection, for retiring hard disk we went and spoke with people in charge, understood their process. They report it back to us, that's compliance component or factor for us.

From the structuration point of view, Kevin is legitimizing the work done by his group to develop the security manual, which is expected to provide a common interpretative scheme to understand the security objectives as applicable to the DOT work

requirements. In evaluating the efforts of the security group, Camila acknowledges that the awareness section is good and “keeps people informed plus it is constant.”

However, she dwells on the importance of good educational communication tool. “We are not there yet in that sense,” acknowledges Camila.

To achieve compliance with the security policy, the IT security program manual required each employee of the DOT to undergo an online security training and obtain a certification of compliance each year. In this case, the norm of obedience is invoked through the facility of control. Through training, the management tends to impose upon each employee a common interpretative scheme to understand the security objectives as applicable to the operational environment of their work. Essentially, each employee had to read the IT security policy and answer a few multiple-choice type questions pertaining to the security policy. At the end of successfully answering these questions, each user was awarded a certificate that recorded the date of completion of online training.

The certificate was in essence a communication medium to signify that all users abide by the security policy and their subsequent actions would be legitimate if they are based upon the understanding of this policy. Although commonly considered as trivial, the online certification tool was used effectively by the security group in promulgating the security program across the organization. The security group decided to use security training to turnoff access of employees who had not achieved the online certification. Wade explains this as management viewpoint where “you can’t manage it that you can’t measure.” For Adam,

Out of 7000 user accounts, 25% of the accounts had to be terminated across the DOT. This kind of result was unheard of at DOT. It convinced everyone about the importance of security.

Such statements indicate a common interpretative scheme being employed to assess the situation and also willingness to understand what IT security meant for the DOT. The security program manual detailed that accounts of such individuals (without certification) should be disabled. However, the security group worked with various divisions to get the number down to thirty-four by June 2007. The access to the accounts of these thirty-four employees was subsequently terminated.

As indicative in the above discussion, training was used as a control tool so that the intent of various employees could be known by way of abiding to the proposed security objectives. The failure to attain an online certification was perceived as a message from a user that she does not share similar signification structures. For such users, the CISO had to exhibit the use of power provided by the security program manual, to turn off access until the user demonstrated obedience to authority. To reinstate their respective user accounts, these employees had to follow procedures, which in the words of the security manager were unfriendly. As per Wade,

If you don't have performance evaluation, people don't care. Such employees with delinquent certifications got notices as annual performance review.

The security group employed the certification facility as a tool for domination and the performance evaluation reviews as control mechanism to signify user non-compliance with shared meaning of security as adopted by the DOT. "This was done to put a message across," justifies Kevin. The CISO was strongly supporting such actions.

According to Adam,

I was ready to terminate the Deputy Commissioner's account if he didn't take certification. Two Assistant Commissioners didn't take it. We gave them two weeks notice. One of them did it and one didn't. I told him you got until midnight to comply. He did it.

However, Adam warns that such actions cannot be taken everyday but need to be asserted when necessary. "Don't keep sending security changes everyday," states Adam. In actual, the human resources division was responsible for the security training program. As the training program was not operational, the security group decided to take it as an extra responsibility, improved it and handed it back to the human resources division upon making the program effective.

Transforming culture by sowing positions of support in organizational silos

Given the nature and size of the DOT as an organization, it was not easy to manage the security program. For Adam,

Security has major holes in adaptation since the DOT is large and diverse both organizationally and geographically. It is not easy to manage the security program in DOT because of size.

He realized that although major responsibility for IT security was still with the Division Heads, there was no one to take care of it. To address this issue, Adam decided to create a position, fund it, and assign responsibility for IT security to that position. In this case, the CISO is employing his facility of resource allocation to create a position. In this regard, Adam had two meetings with the divisional heads to present the security program manual and also discuss the possibility of creating a new position of IT security coordinator. Out of thirty division heads, ten decided to be in charge of security. Kevin explains such decision as,

It is fine whether they delegate or not. The division and district heads are ultimately responsible.

As a result, each division now has one IT security coordinator. The coordinator position was created to minimize tendency to influence security by divisions like audit. For Kevin, the problem of getting IT security coordinator positions was “overcome with negotiation and perseverance.”

The position of IT security coordinator was seen as essential to transform an organizational culture whereby security was considered to be the last thing, although individually it might be considered as significant. Such action signifies that security is generally considered to be unimportant by the organizational members and as such do not share the signification structures of the security group. “Everyone is so busy doing other things, their work, that security is the last thing,” states Paul Simmons, security analyst. The new position of security coordinator was created to sanction the security aspects and be used as a communication source for the respective divisions. The security group wanted to communicate the norms of secure environment as legitimized by the DOT management along with sanctioning specific actions as deemed significant to achieve secure operations. As such, the new position of security coordinator in each division would help in developing a shared vision on how to achieve security. It would be a collective action on part of the division to ensure good security practices, and in the process also helps the security group to ensure a secure environment for the DOT operations. Camila captures the work culture of organizational members at DOT in the following statement:

We are very comfortable with what we are doing, what we always do. Its DOT.

Such lax attitude at work makes Paul to believe that it is critical “to ingrain a corporate mentality that security is important.” This indicates the need to establish the norm of a secure environment for the benefit of the organization. Similar concerns were also brought up by Wade Green who mentioned that it was not uncommon to find computer terminals open while members left desk unattended. Such cases are an indication of a level of awareness and also a level of trust. However, Wade believes that the “level of awareness needs to be higher while level of trust should be justifiable.” The norm of secure environment could be established through the facility of awareness.

Another interesting situation involved the security group to deal with one of the divisions that had trouble as it was out of scope with the security policy on few issues. Citing the problem Camila purports,

There’s a cultural issue here as they never had to deal with central office and security.

However, Kevin did not make much of the problem. For him, adoption of the security policy was considered more like a law at the DOT. This indicates that the policy had been legitimized and was to be accepted by the organizational members. As Camila argues,

They might balk at two points but at higher level they are fine and would get along with it. We have new security policy that is law. They would grumble but would get it done. Culture didn’t stop security here. It did effect and stop my last project.

Both Kevin and Camila suggest that the problems related to organizational culture were successfully overcome by invoking structures of legitimation and domination. The power inherent in authority was effectively used to accomplish the objectives of the security initiatives at DOT.

Attaining security goodwill by paying homage to fiefdom lords

Given the nature of DOT and the fact that it is one of the largest transportation organizations in the country, it would not come as a surprise that the political environment at DOT is generally intense. Brenda humbly put it as “mighty political.” Taking into account the ground reality, the CISO decided to pursue a strategy of making incremental changes rather than one of drastic changes. For a large organization, “it takes time to get people on board,” says Adam. The hierarchy at DOT is such that there is the CEO, the deputy CEO, the District Division Heads and then the Functional Division Heads. The District Division Heads are collectively more powerful than the Functional Division Heads and there is also an informal network among them. They would collectively decide to go in a certain direction or do certain things. The division heads seem to have a good understanding of the structures of domination. The establishment of an informal network indicates successful employment of the facility of coordination among them. By channeling their efforts towards an end they are able to effect control over uncertain situations. For Kevin,

The district heads are little kings. They have autonomous power and can really get in your way.

“You have to understand that there would be conflict of anything that needs to go through across organization,” cautions Camila. As such, it became essential to convince these powerful agents and also to build relationships and network.

The security group faced an uphill task in getting different divisions working together. “Getting everyone to work together at strategic agency level is a challenge,” said Camila. It was problematic for the group to get everybody to agree on a particular

issue and follow the same process. “There’s resistance on any thing that is pushed out from central office,” reminds Kent Davis, the COOP manager. The fact that the CEO had sent a strongly worded memo carried a lot of weight. The security efforts at DOT were laid out as coming directly from the state. For Kevin,

It left no debate. This was a key thing. It took away real case if some District head could take away. For instance, if we had a, b, c, d, e, f, g then e, f, g if not required by DOT would be open for debate.

This understanding of political realities at DOT helped the security group to “take away real case” from the division heads to argue. Essentially, the security group was able to effectively employ the structure of authority to legitimize institution of the security program across the organization. The group was careful to properly communicate the security objectives in the program manual exactly as captured in the state security policy. This allowed the group to further legitimize their endeavors and prevented groups to avoid dominance battles with division heads.

In case of IT security coordinator positions, being a CISO Adam decided to use his control over resources and their allocation to fund positions and assign security responsibility in the division. This was also to help the division heads who were essentially responsible to implement the security program manual in their respective divisions. The CISO gave up the facility of control over these positions to the division heads to avoid any untoward power conflicts. Actually, these positions were charged with the responsibility of dispersing security requirements as communicated by the security group. However, the divisions got sidetracked and started to hire folks with background such as finance rather than IT. When the security responsibility started

trickling down from the security group, the incumbents of the security coordinator position complained that they have lot of work. “Adam and Camila told them that we provided money and you picked the wrong people so it is your problem,” recalls Kevin. From Camila’s perspective, “it is very significant to get things done.” She suggests to give and take favors, and build relationships to deal with the political dynamics at work. “Key factor is, one can’t tell anyone to do anything,” said Camila.

Surviving through security sustenance

The security group took implementation of the security program at DOT as a big challenge. Under Adam’s leadership, the group translated the security objectives into actionable items. Besides costs and risks, culture and resistance to change were evaluated. The group communicated with each other on security objectives so as to arrive at a common interpretative scheme. Further, the need for well-trained employees to maintain the program was also realized. For Adam,

We need strong trained employees to maintain the program whether we are achieving our objectives or not...Daily care and feed for security is critical. Without this, the security program is dead.

The group concentrated on developing skilled process, people and managers at the helm of the security initiatives. Adam guided the security group to approach security efforts at DOT in two phases. In phase one, the efforts were focused on consistent adaptation of the security program. In phase two, the emphasis of the group was on the maintenance and upkeep of the security program. “Most

important thing is security sustenance,” notes Adam. The CISO used the facility of coordination to promote the norm of sustenance that he believed in. The belief in sustenance was communicated to the security group members who focused on achieving similar understanding of the norm.

Given that DOT is a big and dispersed organization with around eight thousand and eight hundred employees, the very size posed a few challenges. The management of technology, policy and practices was complex and also required adequate resources to be allocated by the executive officers through the facility available to their position, as IT security is neither easy nor cheap. For Adam, “if you go skimpy in budget allocation or staffing, you are gonna pay for it.” Despite such a belief, Camila felt she was not provided with adequate resources and time by the CISO. According to her, “things would not be given no matter how many times I go and ask.” Another security group member, Brenda also felt the need for dedicating “more resources to ensure that all bases are covered.” The security efforts involve implementing nine component programs and seven members to make it happen across the organization. However, Kevin disagrees with such views as resources were made available to him as and when needed. Another dimension of interest from sustenance viewpoint is self-enforcement. “You can’t leave it upto someone’s good intentions,” reminds Wade. It is essential to have procedural and automated measures in place that operate to enforce core security practices. The emphasis needs to be on compliance with practice rather than intent of the people. For him, “there should be a mechanism that can’t be bypassed.”

6.3.3 Discussion and summary

The information systems security initiatives were embarked upon with vigor at DOT primarily to abide by the state legislation requiring compliance with the state security policy. This is not to imply that security efforts were non-existent at DOT but they did not involve the seriousness required for such a critical issue. To effectively design the security initiatives, the organization was restructured so as to move the security operations under the control of DIT. Such a move could be attributed to the events unfolding at DOT influenced by the circumstances of both internal and external context. However, it would be prudent for an organization to structure information systems security as a separate department reporting directly to the CEO.

The security program was developed around the structure of state security policy for consistency and efficiency reasons. To address the organizational requirements specific to the DOT, a security manual was developed along the lines of the state security policy but the procedures outlined in the document were configured as per the internal requirements. The aim was to design a comprehensive program which would necessitate all members to observe secure practices without making the program bureaucratic. It is essential to base the information systems security program of an organization on an internationally recognized standard or as evidenced in the case, on a state security policy as required by the law. That is, the policy should address the components advocated in the standard. However, such components maybe fleshed out

as per the business requirements of an organization. Such endeavor would be more reliable and beneficial for an organization rather than blindly adopting a state security policy that might not even be based upon the industry best practices.

Once the security program was developed, the program had to be instituted across the organization. To do so, strong management support was seen by the security group as quintessential for the success of the program. In fact, the CEO wrote a strong memorandum to various division heads emphasizing his commitment to enforce the security program. The effect of such support was seen throughout the implementation phase. There were numerous instances where the security group was able to overcome hindrances or doubts by virtue of the management leadership. The important point to note is strong leadership, which is the critical factor, and not merely management support as has been proposed by prevalent academic literature. A strong leadership displayed by the CEO would invariably entail support across the organization. Perhaps it is a definitional issue in terms of different views, however, there is a difference between leadership and support that makes all the difference.

The security group created awareness of the security program among organizational members. Training was used as a control tool whereby the failure to attain an online certification of compliance was seen as a message that user does not agree to abide by the security policy. Such disobedience with authority was dealt by suspending accounts and bad performance reviews. Although using training, as a compliance stick seems to be an effective mechanism, it should be pointed that the

quality of user training and their resulting understanding about security issues was dismal. It is imperative to educate users on different issues and facets of security and not merely provide them with automated training. An effective information systems security requires education of organizational members where training might be one of the components, and awareness yet another component.

For any initiative to be successful, it is imperative to understand and address the cultural as well as political realities of the organization. Education of organizational members may be seen as one of the ways to transform an organizational culture. At DOT, the security management employed a novel approach to overcome organizational silos by creating and funding the information security coordinator position in each division and district. Such an action may be seen as an excellent demonstration of understanding of the cultural and political context of the DOT by the CISO. This position would not only garner support for the security group but may also be used as an effective informal communication mouthpiece for the group. The availability of an additional employee by virtue of the creation of this position was also a gesture to help the division heads bear the security responsibility. The CISO was effectively able to outflank the organizational politics by initiating a maneuver that restored full control over newly created positions of the information security coordinators squarely in the hands of division heads. In addition, it would also be prudent for an organization to promote participation of powerful agents in instituting security program across the organization. This may be achieved by formally creating a security council with

powerful agents as council members. Such a council would function as an advisory group to the security team.

6.4 Social Transformation at the Department of Transportation

In this section, we employ the theory of social transformation, as advocated by Giddens, to further understand the case study. Barrett and Walsham (1999) note that Giddens' later work actually builds upon the core structuration theory and provides a complete picture of the phenomenon. Giddens later work also had an emphasis on the importance of time and space in structuring of social relations (Barrett and Walsham, 1999). This conception is used to understand the modernity and its transformations. Broadly, the transformation is addressed at two levels – global tendencies and self-identity. Barrett and Walsham (1999) have applied the theory of social transformation to IT domain. The theory has been successful in explaining the link between IT and transformation, as it relates changes in modern institutions to shifts in self-identity.

Although Barrett & Walsham (1999) endeavor to bring in IT as an explicit dimension, we restrict ourselves to the general theory as provided by Giddens. The application and use of the theory of social transformation as an extension of the structuration theory or auxiliary to the structuration theory is consistent in understanding the main research question which deals with how security initiatives get instituted in organizations. In other words, there is a link between an IS security initiative and organizational change or transformation that needs to be explored. The theory of social transformation purports to explore this very link. In essence, we are

viewing this theory as an extension of the structuration theory and following the intellectual work of Barrett and Walsham (1999) in its application in modern organizations.

For Giddens, the globalizing tendencies in modern times derive from three sources: the separation of time and space; the development of disembedding mechanisms; and institutional reflexivity. It is necessary to consider both social relations between people present in time and space, and between those who are absent in time and space. The underlying assumption in modern organizations is the precise coordination of the actions of various stakeholders who may not be physically present at a given place but are nevertheless connected to time of action. The disembedding mechanisms imply the stretching of social relations which allow for the separation of interaction from the particularities of locales. This term is linked to the separation of time and space. In modern organizations, due to separation of time and space, the social relations have been lifted out of local contexts of interaction and reenacted through trust across indefinite spans of time-space. As explained by Barrett and Walsham (1999),

Giddens distinguishes between trust relations that are “sustained by or expressed in social connections established in circumstances of copresence (same time and place),” and the development of trust in conditions of absence as a consequence of expert systems (pp. 4).

Institutional reflexivity implies that there is ongoing questioning and revising of existing knowledge and practices that may also lead to the reordering of existing social relations.

For self-identity, there are three key concepts: concern for deskilling, for existential anxiety, and the opportunity for reskilling and empowerment. In modern

organizations, there is a potential concern for deskilling with the utilization of new knowledge. Further, such utilization would also have an impact on existential anxiety of organizational members. These activities may also result in development of new skills by these members. Giddens suggests reappropriation and empowerment as two alternative possibilities to reskilling. The former is associated with the reappropriation of knowledge and control.

...while people may lose skills and forms of knowledge, they remain skillful and knowledgeable in the contexts of action in which their activities take place (Barrett and Walsham, 1999: pp. 5).

In terms of empowerment, the new knowledge provides organizational members the power to alter the material world and transform the conditions of their actions. As such, the organizational members always have an option between local way of doing things and procedures offered by the expert knowledge (Barrett and Walsham, 1999).

6.4.1 Evaluating globalizing tendencies at DOT

The globalizing tendencies are the result of separation of time and space between entities, the development of disembedding mechanisms and institutional reflexivity. These sources are evaluated in the context of DOT in the following subsections.

Separation of time and space

As mentioned in earlier sections, the DOT has to abide by or comply with the information systems security policy and standard developed by the state technology

agency - ITA. This policy does not necessarily take into account the context of DOT operations. “They shouldn’t go with the approach that one shoe fits all,” argues Adam Martin. The policy had been written by the ITA for all government organizations in the state of Wonderland irrespective of the organizations being either geographically dispersed or their operations heavily dependent upon information.

The social relations are enacted between the ITA and the DOT security teams as the latter have to understand the underlying beliefs of the ITA security team as captured in the clauses of the policy. For Adam,

We could either adopt what they have done or do it on our own. The ITA didn’t do it on their own. They took input. Lot of my folks worked on it.

Further, the policy has to be interpreted and implemented at the DOT. “Because its real world, you do have to tamper policy and standard as per our culture and politics,” explains Kevin Simmons. In a similar manner, social relations also exist between the headquarter security group and various divisions and districts of the DOT who have to abide by the security program.

In addition, IT aspects of security (IT infrastructure) have been consolidated with the ITA and further outsourced to the Outsourcing Firm. The ITA is generally looked upon by government agencies as two organizations, one dealing with governance and policy development and second that support agencies (IT infrastructure via the Outsourcing Firm). As per Kevin Simmons, “that’s a problem for agencies” as they are required by the policy to be responsible for the service provider, “which is ITA who have outsourced it to Outsourcing Firm.” Alex Simmons expressed similar sentiments as well.

Another issue with the ITA is that it is asking the agencies to ensure the service provider [ITA] to protect the systems with proper security. It is frustrating.

Now, the state security policy stipulates the DOT to ensure that the ITA - Outsourcing Firm partnership actually observes good security practices for the DOT related transactions. Here, the social relations are now seen to be extending beyond the ITA and also bringing the Outsourcing Firm into picture.

Development of disembedding mechanisms

The CISO of DOT has to trust that security policy developers at ITA are indeed knowledgeable and working to develop best possible security policy for the state and the DOT. As per Adam Martin,

I like them to look for the practicality of implementation of proposals they are making. ... The ITA should look at operation point of view for security rather than governance and policy only. I think their role needs to evolve to more operational and practical.

Also, the CISO has to trust that the ITA security group is indeed helping them rather than looking for ways to force the DOT to buy services to boost revenues. In fact, Kevin lamented on the “half-baked services” offered by the ITA and how he was “paying a fortune for those services.”

Trust in the ITA got diminished when it extended compliance deadline at the last minute. Kevin was upset with this act of generosity from the ITA. He recalls,

I had to deal with angry district security coordinators. They felt they had gone out of way to get things done. They bugged the District Administrator who thought it (security) was not that critical in first place. My response was that the ITA has extended the compliance deadline but not our Commissioner.

Members of the security group at DOT accuse that significant resources were wasted as they could have achieved the compliance within an extended deadline with greater

efficiency. Then there was an instance of mistrust where members of security team at DOT felt that they were being asked to do the work, which the ITA was expected to do in the first place. Camila Green contends,

It is a very complicated scene. Josh at the ITA was just running us around. They were telling us that DOT you do the work and we take credit for it. Be honest.

Despite such instances, the DOT had to trust the ITA - Outsourcing Firm partnership that they are doing what is required to protect the IT infrastructure. The security team members consider this aspect of the ITA as infrastructure providing organization particularly challenging. Adam attributes the difficulties arising from the ITA's role of IT infrastructure provider as an issue of "struggling with deciding on roles and responsibilities" between itself and other agencies.

The DOT can only rely upon email communication and assurances provided to them by the ITA, as they are not allowed to physically verify the operations at the data center. This lands the DOT as an agency in another predicament as highlighted by Kevin in the following excerpt,

In case of intrusion detection, policy says agency would do monitoring and log. Since we don't own that stuff, it doesn't belong to us and second, we are not dealing with operational side. We have to go and talk with the ITA and the Outsourcing Firm's operations. They said that we don't have IDS therefore there are no logs.

The above statement indicates a lack of control by the security group at DOT over its service provider the ITA and the Outsourcing Firm to get them to do what is expected as per the security policy and the contract. The intrusion detection system should be in place in accordance with the service contract with the ITA. However, this was not the case. The DOT has been exposed to unexpected risk as a result of ITA's 'half-baked

service.’ The irony is that the DOT cannot do much about the situation and has to pay for such incompetence. At the most, the DOT can rely on the summary reports and outputs generated by IT systems that indicate breaches and incident reports. The actual reports per server or subsequent actions taken on incident are not shared with the DOT by the ITA - Outsourcing Firm partnership.

The DOT has to implement the ITA security policy and standard within a given timeframe, as decided by the ITA on behalf of the state. In addition, the technical aspects of IT security (infrastructure and technical employees) have already been consolidated by the ITA although the DOT is still responsible for any untoward incidents. As such, this case is rather interesting and different from a situation where an organization might adopt IT security standard within a timeframe deemed necessary by that organization itself. Generally, organizations would be in control of technical IT security operations, although in some cases security operations might have been outsourced to a third party for resource efficiency. However, in the case of DOT compliance with the security policy and standard was involuntary and forced. The DOT did not have control on the timeframe and technical expertise had already been lost to the ITA as a result of statewide consolidation.

Engaging in institutional reflexivity

At DOT, there is an ongoing questioning and revising of existing knowledge among security members. For the CISO Adam Martin,

Most important thing is security sustenance. We need strong trained employees to maintain program whether we are achieving objective. ... We need dedicated

maintenance organization that would support and keep up with your program. Teams working together are essential. You need a holistic approach otherwise it would be in difficulty.

The security policy requires employees with knowledge on different components of organizational security. At the least, organizational members have to understand components of the IT security policy. These would include risk management, disaster recovery, access controls, and contingency planning among others. Also, the sustenance of security program entails the security group members to be knowledgeable about IT auditing.

The existing practices were scrutinized in the light of the new policy and necessary changes were made to become security effective. To get access to IT systems, there were a number of different ways by which an employee could request access to required IT systems for job related work. The security team worked to consolidate these different access methods into a standard form. For Kevin,

It is a three part deal. One, we need to have standard process for access. Second, standard request forms should be available. Then, automate it for web-based access. All these are ongoing.

To get compliant with the state security policy, the DOT security group requires all employees to have read the information systems security policy. Delinquent employees have been punished by way of suspending their computer access accounts. Adam recalls his tough stance to change the old practices,

I was ready to terminate the Deputy Commissioner's account if he didn't take certification... In one district, there were 12 employees who didn't do it. I called the District Administrator. He told me to terminate their accounts if that's what required to get their attention. I can't do this everyday. But has to do it when necessary.

Few other practices have been revised because of the security policy such as evaluating and classifying data sensitivity; and, formalizing incident reporting. In addition, IT project teams are required to formally think about and inculcate security considerations in their projects. Towards this effect, project teams have to demonstrate to the CIO during presentations that security aspects were indeed considered.

6.4.2 Understanding self-identity at DOT

Self-identity involves the concern for deskilling, for existential anxiety, and the opportunity for reskilling and empowerment. Such concerns need to be understood from the standpoint of DOT organizational members.

Concern for deskilling

The implementation of the security policy requires adequate skill set in IT security. It would require formal training or certification, like CISSP. The successful implementation necessitates both technical and non-technical (organizational) skills. “Have skilled people, skilled process and skilled manager,” asserts Adam Martin. Further, the legislation and security policy requires positions of responsibility to be staffed with people having required degree or certification and proper experience. For Adam,

Other agencies don't like the ITA since they don't have competent technical staff. The DOT has. We have been through this before.

Such confidence of Adam about the competency of his security staff is especially interesting, as half of the security team had mentioned about their handicap in not

possessing proper experience or undergone training in IT security. This observation on deskilling forces us to think about how these members were actually able to conduct their job responsibilities. Such concerns lead us to the concept of reappropriation, which would be discussed after the following section.

Existential anxiety

As has been mentioned earlier, there has been consolidation of the IT infrastructure by the ITA. Subsequently, the network or system administrators were no longer required at the DOT and had to either lose their jobs or move to the ITA - Outsourcing Firm partnership. Alex Simmons is critical about the anxious moments experienced during the uncertain consolidation period. He recalls,

People were basically told that this is what's going to happen, do it or walk away. People moved from the DOT to the ITA to the Outsourcing Firm. The alliance or allegiance was slow to move from the DOT to the ITA to the Outsourcing Firm. There was backward thinking. The ITA didn't have real progressive view. If we consider technology as the main thing for roads and the lack of latest tools, we could say that for every penny spent on technology, not a mile of road has been built.

All this amounts to existential anxiety. At the same time, there were employees who had to upgrade their skills in security or risk losing their jobs.

The employees in security responsible positions (like security coordinators or division heads) at the Divisions and Districts had to take on an additional role of security. This was beyond their main job functions for which they were hired. As per Alex Simmons,

There is a security coordinator in each division and district to help in reviews of compliance. It is extra duty for all. Security is not their full-time responsibility. Generally, the Heads of district and division appoint individual people. For security, there is no rule.

The additional responsibility indeed amounts to existential anxiety. These individuals might have to educate themselves or keep themselves informed about security aspects even though security might not be their primary job function. In addition, employees responsible with security aspects have to comply with the requirement of certification during specific period of time like last three to five years, along with appropriate experience in certain cases.

Reappropriation

The security manager at DOT did not have any experience or background in IT security. According to Kevin,

I am an IT project manager. Adam never intended for me to do the security manager role. I go from idea stage to get it running and then move on.

However, he became knowledgeable about security while trying to implement it at the DOT. Only deputy security manager and one of the security analysts, Paris Simmons, were knowledgeable about security to an extent, the former because of his experience while the latter by virtue of her education. Alex attributed this problem of lack of appropriate human resources to the consolidation by the ITA. For him,

With formation of the ITA, it took security people away from us. The ITA has job and people but agencies have the responsibility. We had to do it without people and resources.

In fact, few members of the security group initially avoided the interviews conducted during data collection for this research and tried to avoid specific security questions.

They would appreciate job related or more general questions. Despite the handicap, the

team members remained skillful and knowledgeable in the context of their job requirement to develop and implement a particular component of the security policy. In fact, the security manager approached security initiative as a project.

Empowerment

The security members altered the operational environment at DOT by introducing new practices for the organizational members. By observing such practices, the organization members would in fact lead to secure operational environment. A classification system for information is generally recommended by various industry best practices. However, such a practice has not been adopted at the DOT. This particular concern was vigorously pointed out by Wade Green during a meeting. In his words,

There's no policy or document that defines marking of documents as classified, officials only, etc. Once you have those rules, implementing and ensuring them in automated system is trivial. There's no system in place for information security classification and handling. How do we know which information is hazardous to agency? That's the biggest gap.

In fact, Wade is more concerned with the general consent among the group as not to go “beyond statutory requirements.” Such an approach for him has resulted in a situation where there is “no documented set of procedures that would allow anyone to handle an item of information.” However, such practice is followed because of the nature of the organization. Since the DOT does not deal with a lot of sensitive information it does not make sense for the organization to classify all information as per some classification system. The sensitive information that the DOT does possess may be requisitioned through the Freedom of Information Act. The security group adopted and reconfigured

the advocated security policy and standard, and best practices as per the requirement at DOT. This can be seen as selection between local way of doing things and procedures offered by best practices.

6.4.3 Discussion and Summary

The CISO guided the security group to initially focus the efforts on consistent adaptation of the security program, and later support it with strong maintenance and upkeep of the security program. To take the security program to a level of maturity, the emphasis has to be upon developing skilled process, having skilled people and skilled manager at the helm of the security efforts. Skilled process and people requires understanding the nature of modern organizations that are influenced by globalizing tendencies and concerns of organizational members at the individual level. At the institutional level, there is a separation of time and space among different agents and projects which necessitates adequate attention to the social relations between such parties. In the case of DOT, the security group had to understand the underlying beliefs of the ITA security team as captured in the clauses of the policy document as it was not written specifically for context of the DOT. Further, the social relations were seen to be extending beyond the ITA and also bringing the Outsourcing Firm into picture. Such might be the case for other organizations as well where various teams involved in different facets of the security program might not have the opportunity to interact directly with one another. One team might be involved in configuring the standard

based upon the policy developed by a standard developing body. In such cases, it is essential to maintain the social relations through trust across the dimensions of time and space.

At DOT, the CISO had to trust the security policy developers at ITA that they are indeed working to develop best possible security policy for the state. There is a chance that this might not be the case in reality. Also, the DOT had to trust the ITA - Outsourcing Firm partnership that they are doing what is required to protect the IT infrastructure. In some instances, such trust relations were in fact suspended especially in the case of extending the policy compliance deadline. In yet another instance, an apparent lack of control was evidenced by the security group in its inability to hold their service provider, the ITA - Outsourcing Firm, to the agreed upon commitments. These instances indicate the importance of developing trust relations as disembedding mechanisms in the organizational practices. At the same time, the existing practices need to be questioned and revised at regular periods of time. At DOT, the existing practices were scrutinized in light of the new policy and necessary changes were made to become security effective. In fact, few of the practices changed involved developing standard practice to get access to IT systems, evaluating and classifying data sensitivity, inculcating security considerations in IT projects, and formalizing incident reporting.

At the individual level, the security management needs to be sensitive to the self-identity issues of organizational members to institute the security program in an organization. The effective implementation of the security program requires adequate

skill set in IT security, which might trigger concerns for deskilling. In addition, the new requirements might place additional responsibility on specific positions or might as well render them unnecessary. As in the case, an organization perhaps might decide to consolidate or outsource IT infrastructure. Such instances would inadvertently create an existential anxiety among organizational members. It would be prudent to address such concerns ahead of the curve and take appropriate actions to minimize potential discontent among employees. Such discontent is widely considered in the prevalent literature to be a major factor for computer crimes or weakening of security defenses.

In case where a team lacks significant human resources, it might be helpful for the management to tap and emphasize the inherent learning capability of organizational members. This was adequately demonstrated in the case of DOT whereby the security manager and security team remained skillful and knowledgeable in context of their job requirement to develop and implement the security program. The security members altered the material world at DOT by introducing new practices for the organizational members. In fact, they consciously selected between local way of doing things and procedures offered by best practices. An organization would be adequately served by nurturing and grooming the employees with particular value set that imbibes responsibility in effecting changes, learning capability to re-skill, and intelligence to understand the changing organizational context.

6.5 Discussion

The analysis of empirical evidence from the Department of Transportation case indicates certain factors that seem to play an important role in instituting an information systems security program in an organization. The implications for information systems security from these factors are summarized in table 6.1. These implications may be significant in varying degrees, dependent upon context, in strategically transforming an organization to a higher level of maturity in terms of information systems security.

At the strategic level, the learning from the empirical analysis may be summarized visually as a model, which is based on Sarason's (1995) model of strategic transformation. Sarason's model, however, did not include components of the theory of social transformation as advocated by Giddens. We argue that incorporating globalizing tendencies and self-identity is necessary to provide a deep and thorough understanding of the phenomenon of transformation in terms of strategic information systems security in modern organizations. Sarason (1995) argues that the structuration theory offers strategic management a theoretical framework to understand strategic transformation. The author integrates the concept of organizational identity with the structuration theory to yield insight as to why a firm adopts a particular strategic path.

Table 6.1: IS security implications from structurational analysis

Emergent issues	IS security implication from case study
Organizational structure bias	Structure IS security as separate department reporting directly to CEO.
Developing security program content	Security policy based on national or international standard or law.
Need for security conformity	Strong management leadership, not only management support.
Creating security awareness	Education of organizational members, not only training.
	Online certification as compliance stick.
Culture conducive to security practices	Creating and funding positions of support to overcome organizational silos.
	Respecting and involving powerful positions of authority.
Effective security processes	Sustenance of IS security program through strong maintenance and upkeep.
Security related globalizing institutional concerns	Maintain social relations between security teams at all time and over space.
	Develop trust relations as disembedding mechanisms between different security agents.
	Institutional reflexivity revising existing practices and knowledge to develop security effective practices.
Identity concerns at individual level	Need for organizational members skilled in security.
	Reduce existential anxiety due to security through manageable responsibility structures.
	Reappropriation by providing members with opportunity for continuous security education to remain skillful and knowledgeable on job.
	Security agents be empowered to effect change.

The integrated model (figure 6.2) offered by Sarason provides alternative explanation to debates such as strategy and structure, and determinism and choice in strategic management field. For the former, the theory provides

an elaboration of how strategy influences structure in intentional and unintentional direction as well as a recognition of the enabling and constraining influences of structure on strategy. To the determinism/choice debate the framework recognizes the role of intentional action within constraints and without assuming managers have unconstrained choice (Sarason, 1995).

As per Sarason (1995), the understanding of the recursive nature of structure and agents would help focus managers' attention on the translation of intention to structural change.

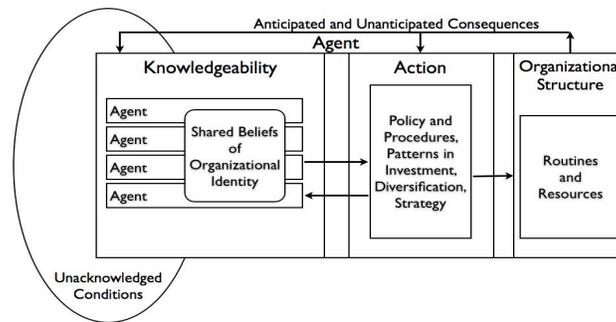


Figure 6.2: Model of strategic transformation (reproduced from Sarason, 1995)

Sarason's (1995) model of strategic transformation is a theoretical endeavor at employing the structuration theory to explain organizational change. Based on the empirical evidence presented in this chapter, the updated model of strategic organizational transformation is presented in figure 6.3. This model helps explain the phenomenon of organizational change to inculcate strategic information systems security concerns in modern organizations as it integrates the concepts of modernity as proposed by Giddens. In the rest of this section, we explain the conceptualization of

different components of the model of strategic security organizational transformation (MSSOT) in the context of information systems security initiatives.

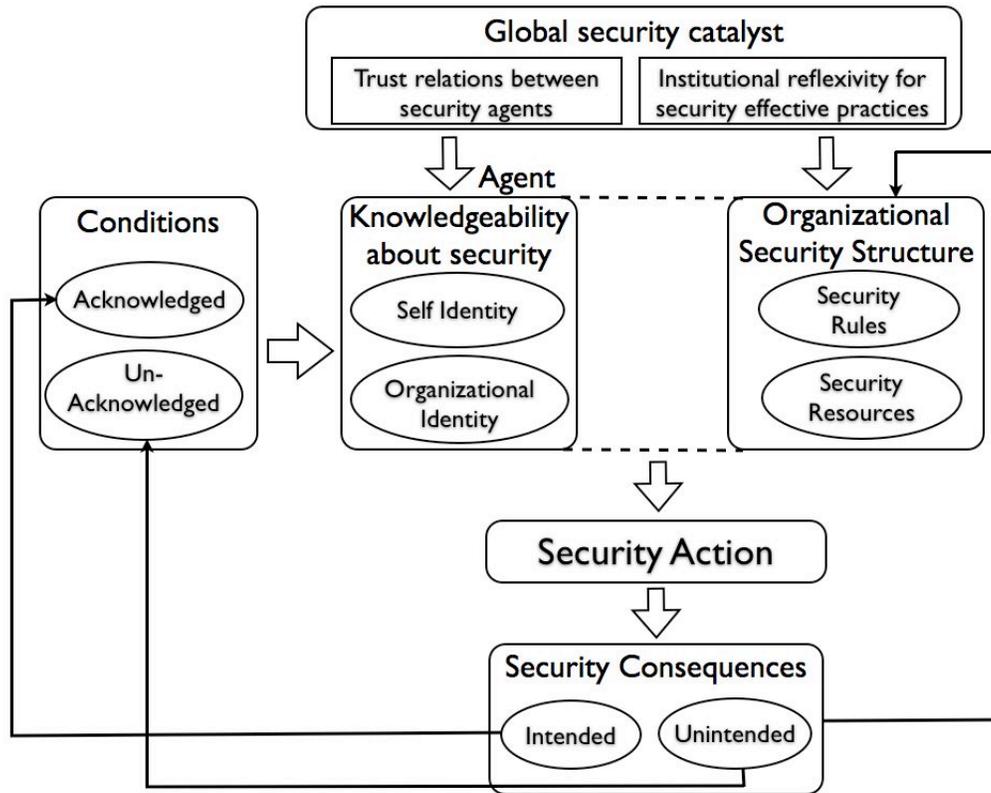


Figure 6.3: Model of strategic security organizational transformation

Security Agent. As evidenced in the case study, security members were purposeful, knowledgeable, reflexive and active. These members were aware of the organizational rules and understood the conditions and consequences of their actions. They used their knowledge in developing and subsequently instituting the security program. Knowledgeability has been demonstrated in the many skills displayed by the security members as part of day-to-day encounters and activities to overcome the

cultural and political realities at DOT. The manager of the security group consistently monitored group's behavior to understand the actions that were being taken and situating them in the organizational context. Such reflexive monitoring was also exhibited by the CISO as he modified actions of the security group to overcome hurdles. This also indicates that a security action is in a way dependent upon the security related knowledgeability of the agents. An action would be monitored by the agent thus affecting her knowledgeability. Hence, a dependency exists between the agent and structure. The security group is situated within the structure and is part of the social system of the specific organization.

Organizational security structure. Security structures are the organizational security rules and resources that agents draw upon and reestablish in everyday activities. These structures are only present virtually as mental traces, that is, they do not have material existence per se. Hence, structures do not exist independent of the agent. These security rules are present in the mind of the organizational members and exhibited through various organizational practices. Inadvertently, the organizational security rules are further confirmed through practices. Such a dynamic approach to structure is consistent with the socially constructed view of an organization.

Unacknowledged conditions and unanticipated security consequences. A security action is bounded by existing conditions, both acknowledged and unacknowledged, and results in outcomes that were intended as well as unintended by a security agent. The unintended consequences from a security action give rise to conditions that might go unacknowledged since such an outcome was not expected in

the first place. Unacknowledged conditions might inhibit future security goals from being achieved, as management would not be able to take these into account. Sarason (1995) provides explanation for such discrepancies,

placing the strategic change process on a time continuum, managers can be seen as setting intentional events into motion. However, because there are multiple agents and unanticipated consequences, change in the social system will appear to have non-rational elements, which influence managers to set into motion a new set of events (pp. 49).

The impact of consequences from security actions on conditions would explain the gap between the desired strategic security outcomes and the real outcomes.

Knowledgeability about security. Sarason used the concept of self-identity for the inclusion of organizational identity in the strategic transformation theoretical framework. However, self-identity was not exclusively included in the model. The discussion on the concept of modernity by Giddens emphasizes the importance of understanding self-identity. It is indeed created and sustained through reflexive activities. The concerns for security related deskilling, existential anxiety and reappropriation are indeed legitimate concerns for members of modern organizations. The demands of information systems security discipline require skilled members who are also able to update their security skills on a continuous basis with the changing IT environment. These do have significant impact on the strategic path undertaken by an organization.

Organizational identity involves a set of shared beliefs that organizational members hold about their organizations (Sarason, 1995). It involves shared values and assumptions about the organizational security posture which would guide the agents to adopt certain actions over others. Sarason (1995) argues that organizational identity

have a dramatic impact on strategic actions of the organization as agents shared belief of her organization (image) as conservative and risk averse would encourage avoidance of risky action. It might be the case that such an aggressive security action might be the need for the hour. However, shared assumption of an organization might keep the security agent from acting in a manner conducive to achieve security goals.

Global security catalyst. Globalizing tendencies influences the modern organizations and it becomes necessary to address such concerns. The management of an organization has to address the separation of time and space in security operations. It necessitates the development of trust relations as disembedding mechanisms between security agents and engage in institutional reflexivity to develop security effective practices. The globalizing tendencies have an impact on how security agents perceive the social organizational world. Their subsequent actions would be based upon such perception of organizational context. At the same time, the security related globalizing institutional concerns would lead to new rules of competition and renewed understanding of organizational security rules by the members.

Link between security identity-structure and security action. A security action is the result of interaction between organizational members. The security related knowledgeability possessed by an agent interacts recursively with the constraining security structures to produce the desired action. The appreciation of self-identity and an understanding of organizational security identity provide constraining guidance to any security action. Such strategic security action impacts the identity through the conditions formed as a result of consequences. In the context of security, an action

might amount to development and implementation of the information systems security objectives, policy, standards, guidelines or procedures. It may also involve implementing security controls and measures to check adverse information related behavior. Essentially, any and all actions required to institute a security program in an organization would become the focus of security action component.

Link between security consequences and organizational security structure. The consequences of security action as part of a desired strategy would have an impact on the security structure. An action reflects the security rules and these are either reaffirmed in an action or new security rules are enacted by way of practice. A security action is brought about through the utilization of resources. At the same time, such a security action might generate more resources for an organization. In either case, resources are changed through an actions of the security team.

The model of strategic security organizational transformation effectively explains the strategic information systems change adopted by an organization. The global catalysts and concept of self and organizational identity renders power to the model to be applicable in modern organizations.

6.6 Conclusion

This chapter has described how information systems security initiatives were developed and subsequently instituted within the Department of Transportation from a structural perspective. Such an approach is argued to be conducive in developing appropriate processes to support information systems security initiatives in a given

context. The analysis in this chapter has evidently shown the effectiveness of Giddens structuration theory, as well as, the theory of social transformation to explain the intricate links between content, process and context of an organizational security change. Based on the emergent issues, a model of strategic security organizational transformation has been developed. The management of an organization needs to pay careful attention to various theoretical components explicated in the model before embarking on information systems security initiatives. This model would assist the interested parties in effecting a successful security change in modern organizations.

CHAPTER 7

Interpreting Strategic Information Systems Security Initiatives in Organizational Setting

7.1 Introduction

In this chapter, empirical data from the ITA and the DOT is analyzed to understand inherent issues that have an impact on the success or failure of an information system security initiative in an organization. The ITA has been developing a security program for a statewide implementation at Wonderland. The organization has witnessed quite few changes since the time such an idea was conceived. The DOT had relatively more success with development and subsequent implementation of the security initiatives. Once the content of a program has been developed, organizational processes need to be set in place so as to achieve the desired results. The problem is to enact the content through various practices within a specific context. As a result, appropriate strategies of action need to be formulated to achieve security objectives of an organization. An action analysis would help explore the inter-relationship between content and processes, while giving due attention to the context.

This chapter is divided into six sections. The next section describes the concept of first-level constructs and second-level constructs. Section 7.3 provides an analysis of

information systems security initiatives at ITA and the subsequent section discusses the security initiatives at DOT. Section 7.5 identifies the emergent issues for discussion. Finally, section 7.6 concludes the interpretation of strategic information systems security initiatives in an organization.

7.2 Understanding Schutz's Concept of First-level Constructs and Second-level Constructs for Social Theory Formation

Lee (2004) considers Schutz's concepts of first-level constructs and second-level constructs as an ingenious device to account for the social dimension of social theory. For Schutz (1954), the individuals in a social setting employ common-sense constructs to interpret the world that surrounds them and "experience as the reality of their daily lives." This common-sense knowledge of everyday life influences an individual's motive behind an action. "The constructs involved in common-sense experience of the inter-subjective world in daily life are the first-level constructs" (Schutz, 1954). It is pertinent that any explanation about the organization should consider the subjective meaning of the actions of members who collectively are considered to form that organization. These subjective meanings are the objective reality that a social scientist intends to study (Lee, 2004). In order to understand the social reality of organizational members, the social scientist would have to develop constructs that are based upon the common-sense constructs held by the members of that organization. These constructs formed by the social scientist are referred to as second-level constructs since they are essentially, as explained by Schutz (1954),

“constructs of the constructs made by the actors on the social scene.” The second-level constructs may be considered as a social theory since these are based upon first-level constructs that “exist in the empirical subject matter of social science” (Lee, 2004).

Van Maanen (1979) uses a similar notion in discussing organizational ethnography although the terminology used is slightly different. For Van Maanen, the facts of an investigation are the first order concepts (similar to Schutz’s first-level constructs). These involve descriptive properties of the studied scene and the interpretations used by organizational members to account for those properties. The second-order concepts are the theories used by the fieldworker to explain the first order data (Van Maanen, 1979). The explanation of the second-order concept is similar to Schutz’s (1954) explication of second-level constructs as the “theoretical systems embodying testable general hypotheses.”

In subsequent sections, Schutz’s concept of first-level and second-level constructs is used to present findings from the ITA and the DOT. Such conceptualization would enable making sense of the inherent complexity of the social organizational setting. This would allow us to account for the “social dimension of social theory,” borrowing Lee’s (2004) terminology, pertaining to information systems security change.

7.3 Strategic Information Systems Security Initiatives at ITA

The following discussion is based on the empirical evidence presented in chapter 5. The information systems security initiatives at ITA were the focus of analysis.

7.3.1 First-level findings

The security initiatives were developed at ITA to address the need of a common information systems security program in order to establish base security practices in state government organizations across the state.

A common information systems security program

The security department at ITA decided to have a common information systems security program for all state government organizations. Such a decision was based upon the requirement of legislation to ensure secure operations for the state citizens. The state government enacted a legislation to introduce information systems security program across the state. The security department at ITA was empowered to develop the information systems security policy to be complied by all state government agencies. The department was also allocated responsibility to develop supporting information systems security standard and guidelines. Essentially, the security department was expected to direct the state in its security initiative, as the Governor and inadvertently the CIO of the ITA were made responsible for any adverse IT incident.

The management team of security department formed a committee to develop various policy, standard or guideline documents. The guideline documents were initially developed by the departmental subject area in-charge and subsequently reviewed by other committee members, which included the Deputy CISO, the security manager, external consultants, and an internal policy expert. In these meetings, committee members were encouraged to freely express their opinion. The security departmental members would openly acknowledge apparent problems in the security policy. The members would also lament upon their adverse relationship with other agencies by making statements such as ‘they hate us,’ and expressions of frustration with the government process. The members were able to express their views in presence of the Deputy CISO, which shows a strong environment of free expression for individuals. The management team was able to effectively channel any negative feelings among members towards developing guideline documents by making them initial owners of such guidelines.

Establish base security practices

The security program was aimed at achieving base security practices in all state organizations. To do so, the government agencies were required to get compliant with the state security policy within a specific timeframe. This would allow establishing a basic level of security practices across the state and help build a platform for secure operations. Future efforts to create secure information related environment in the state could be built upon such a platform.

The ITA has claimed ownership of developing the information systems security program that includes the security policy, standards and guidelines. Any modifications to the security program or policy documents can only be made by the ITA security department. The stakeholders at various government agencies can provide suggestions and comments. However, the final decision on those suggestions is the authority of the ITA. In essence, the security program is developed and monitored by the ITA security department. All agencies are mandated to implement the security program and get compliant with the security policy requirements by a particular deadline. This is essentially the governance role that the current CISO aspired for.

Emergence of governance role

To be effective, the current CISO changed the existing reporting structure such that she would be able to directly report to the CIO. Next, the compliance and governance functions were made prominent. Such emphasis resulted in the merger of security and audit divisions of the ITA. The role of ITA security department emerged to be concerned with governance rather than technical security aspects. The security department developed an information assurance program to portray its emerging role of governance function. In this endeavor, the ITA decided to help agencies by providing expertise for clarifications on implementing different components of the program.

Emphasis on user education and training

The CISO became familiar with the ground realities of state government agencies. In most agencies, the individual in-charge of security did not have much understanding or knowledge about information systems security related aspects. Also, security responsibility for them was in addition to their main job function. To address these issues, the CISO emphasized user education at every opportunity possible. She required explanatory paragraphs in the security policy, standard and guidelines so that non-security personnel could make sense of the requirements. Such efforts were primarily taken to protect individuals from hurting themselves by making bad decisions in terms of information systems security. Ignorance of users was not to be accepted as an excuse for circumventing the state security policy compliance.

To achieve a common understanding of security across organizations, the ITA security department decided to develop a training program for newly appointed CISOs at different agencies. In actual, the security-training component of employee training was taken over from the Human Resources department. The security department then revamped the program so as to expose the CISOs to the department's approach to security.

Tactful engagement of agencies to attain security interests

The organizational members at ITA security department have been very cautious about expressing negative feelings. Although frustrated with the efforts to increase government agency participation, the security department did not express the concerns

directly to various agencies. In private, however, security executives seem to be skeptical about the success of the program with the agencies. Nevertheless, these executives were generally upbeat and confident about the security program with the government agencies.

The SAG meetings were developed as a forum to initiate dialogue between security officers and members of the security department. The aim was to receive feedback on security initiatives developed and also to serve as communication tool for sounding future developments. The CISO pushed members of the security department to help government organizations that were small in business operations. The aim was to help these small agencies because many of them did not even have any dedicated IT staff. To protect self, the CISO of the ITA interacted with the management of bigger agencies (big in terms of size of operations). Such a step was necessary to protect against the political power of big agencies. To win over the support of political heavyweight agencies, the CISO decided to form a Security Council that would serve as an advisory board to the ITA security department. The newly formed council was indeed comprised of representatives from the heavyweight agencies.

Extension of the state security compliance deadline

The ITA security department required government agencies to be compliant with the information systems security policy by a particular deadline. A substantial period of time, about a year, was provided to the agencies to ensure compliance. It must be noted that the ITA required compliance with the security policy only and not security

standard or guidelines. The security department anticipated difficulties with smaller agencies in implementing the state security policy. Various agencies had already protested about the constrained timeframe.

It was not difficult to anticipate that many agencies would have trouble getting compliant by the deadline. The CISO held private meetings with the heads of different agencies to assess the situation. Finally, the deadline was extended on the last day to help agencies not default on the state legislation. However, the CISO withheld information on compliance extension till the last minute. Such a position was justified since the intent was to protect individuals and agencies. The logic followed by the CISO was that agencies would try hard to get compliant with the state security policy. Whatever is achieved in terms of implementing the security policy would be good for protecting an agency to an extent.

7.3.2. Second-level findings

In this section, the second-level findings pertaining to the information systems security efforts at ITA are presented and explained.

Security program as constitution of the meanings and intentions of actors

An action is to achieve certain consequences. Actions undertaken at the ITA were to develop a common information systems security program in order to establish base security practices in the state. Argyris and Schon (1974) argue that an action may be assumed to be designed by an actor. It flows from this assumption that action is

constituted by the meanings and intentions of actors. The security initiatives at ITA can be understood through the theory of action. For Argyris and Schon (1974), there are two kinds of theories of action - espoused theory and theory-in-use. The former is theory that an actor claims to follow. The theory-in-use is the theory that actors actually use and can be inferred from their actions. “Theories-in-use are the often tacit cognitive maps by which human beings design action” (Argyris Putnam, and Smith, 1985). The aim is to assist actors in developing more sympathetic world to their desired intentions.

The model of theory-in-use is presented in figure 7.1. There are three main components in the model – governing variables, action strategies, and consequences. Governing variables are the values that actors seek to satisfy (Argyris Putnam, and Smith, 1985). There are four governing variables, which can be perceived as having preferred range.

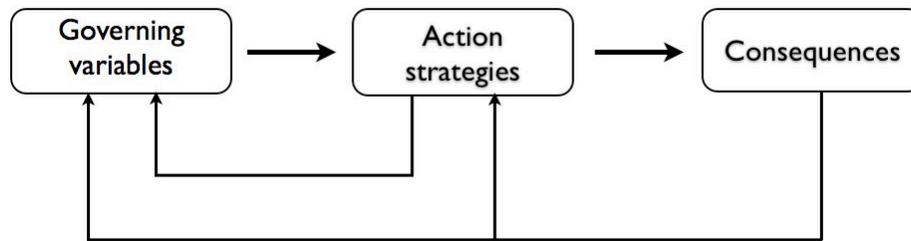


Figure 7.1: Theory-in-use model

(reproduced from Argyris, Putnam and Smith, 1985)

For the ITA, the governing variables for security development include developing a common information systems security program, establishing base security

practices, all government agencies to get compliant, exhibiting confidence in the security program, and providing substantial period of time for compliance with the security policy. Action strategies are considered to be a sequence of moves used by actors in particular situations to satisfy governing variables (Argyris Putnam, and Smith, 1985). These are designed to achieve desired results that will satisfy governing variables. Previous section provided actions followed by the security group at ITA to support the four governing variables. These strategies of action are also summarized in table 7.1.

Table 7.1: Unilateral control model for security development at ITA

Governing variables	Governing variables for security development	Security development strategies of action
Define goals and try to achieve them	Common information system security program	Enacted a legislation; develop the security policy, standard and guidelines; CISO changed the reporting structure for direct access to CEO; compliance and governance function made prominent.
Maximize winning and minimizing losing	Establish base security practices; all agencies to get compliant.	Ownership of developing the security program; agencies to implement security program; establish governance role; developed information assurance program; training program for newly appointed CISOs.
Minimize generating or expressing negative feelings	Exhibiting confidence in the security program.	SAG meetings; help small agencies; CISO interacts with big agencies; formation of security council; channel any negative feelings by making members initial owners of guidelines.
Be rational	Substantial period of time for compliance with security policy only.	CISO emphasized user education; Compliance deadline extended; CISO withheld information on compliance extension till last minute.

Interpreting intended and unintended consequences for single-loop learning

An action would have consequences that may be intended or unintended.

Argyris Putnam, and Smith (1985) explain that unintended consequences may very well

be counter-productive to the desired consequence. In case of unintended results, the actor develops new action strategies to achieve the desired outcome. That is, the actor is still working to satisfy the existing governing variables (Argyris Putnam, and Smith, 1985). This case is referred to as single loop learning as changes have been made only to the action strategies. Since all consequences eventually feed back into action strategies and governing variables, it becomes important to understand the consequences of actions at ITA in order to effect single loop learning.

Manipulative tendencies of the ITA security management

The consequences of actions developed for the state pushed the security department on defensive whereby it was seen as cajoling agencies to participate and provide comments on the security program. ITA was recognized to be competitive by developing a security program that encompasses best security practices from the industry and the National Institute of Standards and Technologies (NIST). The new security program was better than the pre-existing security programs at various agencies. At the same time, the intent of the security department at ITA was to have control over agency operations through compliance and auditing. However, inconsistency lies in the promised goal of program based on 'best practices' and the manner in which it is actually developed. Although the program is based on NIST guidelines, the process of adapting these standards to the requirements and needs of the state is done in an ad hoc manner. A review of the policies and guidelines indicate considerable misrepresentation of best practices.

The security department members were afraid of criticism about job not being done appropriately. The group has positioned itself strongly as experts, bringing in a few academics and consultants to represent or portray an image of expertise. The CISO manipulatively used politics to win over and increase participation of agencies in the process. However, the security department withheld relevant information and did not directly inform agencies that their programs are inadequate. It proceeded cautiously and was slowly influencing agencies to support the common security program.

Defensive interactions of the ITA security group

The state government agencies are dependent on the ITA security department to understand their contextually driven requirements. The problem is that agencies, especially the smaller ones, do not have individuals with appropriate experience or knowledge about security aspects. Now, all agencies are mandated by law to get complaint with state security policy. The defensive positioning of ITA security department is evident in the decision that it has the say in selecting the organization that would audit the agencies. Further, only the ITA security department would approve an exempt status for any exceptions with policy compliance.

To complicate the matters, the auditing agency might not audit agencies based on the security standard developed by the ITA. An independent audit is generally done for the state. In such a case, agencies are left on their own to figure out how to set up adequate security processes and get compliant with the policy. There seems to be little real help extended to agencies although the ITA security department claims to the

contrary. There is a lack of team of experts who might be available to an agency and help them in instituting the required security changes. The ITA security leadership is defensive about such an action and certainly do not want to do agencies' work. The ITA security department has lately emerged to don the role of auditors or the ones policing the state security environment.

Defensive norms influencing the security initiative

The state government agencies feel that the ITA does not have their best interests in mind. There is a general mistrust between the agencies and the ITA, as the former believes that the security initiatives are a way to generate more revenue for the latter. Agencies also complain that the ITA took away control on security decisions while agencies were left to provide for the financial support. Further, the security department of the ITA displayed conformity with a formal method of developing policies and guidelines. The departmental members were simply doing things to appease the CISO and not necessarily the right thing. There are acknowledged issues with the security policy that have not been rectified. In addition, external commitment was sought from the state government, consultant teams, and heads of prominent heavyweight agencies. The CISO has been employing diplomacy to consistently chat up with officers of these agencies during monthly SAG meetings, while her staff engages with officers of smaller agencies. Even formation of the Security Council with members from few heavyweight agencies has an underlying motive to empower the CISO.

Risk averse attitude for security initiative

The agencies have little freedom of choice as they have to abide by the state security policy and live with the decisions made by the ITA security department. In addition, the department itself does not want to take risks. Any changes made to the policy by the security team needs to be commented upon by agencies through an online document system. This might be a mean to provide evidence of participation or hearing their voice. Further, the security team was evasive of adopting prominent international standards. The CISO was also defensive about sending teams to get the perspective of an agency. She was fearful of creating misunderstanding or give more power to agencies. At this stage, the CISO would not allow anything that might stifle support from agencies.

The policy compliance deadline was extended to help the agencies. Although relieved, agencies were upset about the manner in which the CISO extended deadline at the last minute. There were few agencies such as the Department of Transportation that felt betrayed with the compliance extension. In such a case, the ITA faces the danger of being mistaken as an entity with little commitment to see its decision through. At the same time, ITA may be seen as not taking any risk because non-compliance of agencies would end up looking bad for itself as well.

The underlying behavioral strategy for the theory-in-use is unilateral control over others. Such behavior was evident at the ITA security department. There was little public testing of ideas and as such effective learning did not take place. The hypothesis that people generate tends to become self-sealing (Argyris Putnam, and Smith, 1985).

This leads to escalation of error while ineffective problem solving and execution of action persists. The development of effective security initiatives was crucial for the security department and consequently members were most oriented to protect interests of the ITA.

Explicating the espoused theory of security initiative developers

Argyris Putnam, and Smith (1985) emphasize that the theory-in-use and espoused theory is not about making distinction between theory and action. But rather the distinction is being made between two theories of action, one that actors espouse and other that they use. Such a perception is tied back to the assumption that all actions are a result of actor's design. When the espoused theory and theory-in-use are consistent it leads to intended consequences. However, a gap or mismatch between the espoused theory and the theory-in-use would not provide desired results. An actor is generally only aware of the espoused theory, as this is the one she claims to follow.

The espoused theory involves four governing variables. These values that members seek to satisfy include participation of everyone in defining purposes, everyone wins and no one loses, express feelings, and suppress the cognitive intellectual aspects of action. At ITA, the CIO and the CISO encouraged participation of all stakeholders for defining the information systems security program including the security policy, standard and guidelines. Once the security department developed the policy, standard or guideline document it was made available to the stakeholders across the state through an online document system. The users from all agencies would read

the documents and provide their respective feedback pertaining to issues, concerns or further improvement. In addition, the SAG was created to promote participation of all security officers of government agencies in security program of the state.

At ITA, the emphasis was to establish base information systems security practice in all agencies so as to achieve a secure environment for the state. Such a goal seems to emanate from the second governing variable of the espoused theory, which is to ensure that everyone wins and no one loses. All state government organizations were to get compliant with the information systems security policy developed by the ITA. There were to be no exceptions. This is to ensure establishment of a minimum set of secure practices in the state.

The CISO was interested in creating an environment where stakeholders of the security program would be able to freely express themselves and have a dialogue. The SAG as a forum emerged to attain such a goal. Within the security department, the management aspired to have free expression of opinions by the department members. The value of suppressing the cognitive intellectual aspects of action had implications for the security policy. The CISO pushed the security department members not to focus on the best possible security policy but rather to develop a quick and workable security policy. Such a policy should help establish a base security practice in all organizations irrespective of the nature or size of its operations.

Understanding double loop implications

An agent performs an action to achieve desired consequence. If the result of such an action is what an actor intended or there is a match, the theory-in-use of the actor is confirmed. However, if the results are unintended there is said to be a mismatch or error (Argyris and Schon, 1974). Generally, the actor would try to develop new action strategies to correct the mismatch. In case the actor changes the existing governing variables we would refer to it as double-loop learning.

The deliberative process appropriate to double-loop learning is concerned not with choosing among competing chains of means-ends reasoning within a given set of standards, but with choosing among competing sets of standards (“frames” or “paradigms”) (Argyris and Schon, 1974).

The problems that cannot be discussed are the source for double loop issues. If problems persist despite efforts to address them, the situation would require double-loop learning so as to solve the issues. The incongruence between espoused theory and theory-in-use results in a gap that exists in organizational practices. Basically, the intentions of agent are not effectively transformed into action to achieve desired outcomes. This was certainly the case at ITA.

The espoused theory of security management team is to imbibe participation by stakeholders in defining the security policy, standard and guidelines. The security policy was based on the security standards of NIST. However, the NIST security standards do not address information systems security management issues completely. As a result, the security policy developed by the ITA is riddled with issues. Interesting point to note is that the external consultant for security group did suggest the management team to base the security policy on the international security standard

ISO/IEC 17799 Code of Practice for Information Security Management. However, management did not agree with his recommendation. This may be due to the fact that majority of the security departmental members do not have significant security experience. This is especially true with the senior officers of the security department. Most of the departmental members had prior experience in fields other than security such as auditing and emergency management. Few odd departmental members with security experience seem to only appease the CISO although privately they do acknowledge problems with the policy. These members argue that the real need for the state is to establish base security practice in all organizations while the security policy can be improved during the second phase in the following year.

The implication of such incongruence is that error keeps on escalating through all these mismatch generating actions. However, the gap due to incongruence has gone unnoticed by the ITA security members. All subsequent efforts to institute the security program in government agencies are based on a faulty or an incomplete security policy. In case the security policy is indeed revisited, any significant changes made to the policy would seem to waste resources utilized during the current efforts. Further, actions by the ITA security department are simply being taken as situations emerge rather than developed in a cohesive manner or following certain logic. For instance, a query was raised by an agency about how to deal with folks using their own computers to get the job done as part of telecommuting. The security group realized that they did not take this situation into consideration earlier and simply decided to develop a

guideline that could be followed by interested agencies. Overall, there is no real participation of stakeholders in defining the security program.

The approach so far for the ITA has been to adjust action strategies when intended consequences were not achieved. Such an approach can be problematic as only single loop learning takes place. In order to address root problem of the issue we would have to reconsider the governing variables. A re-evaluation of governing variables with adequate consideration to the espoused theory would effectively address double loop issues. At ITA, implementing the information systems security policy in all government agencies across the state was part of the espoused theory. In observing ITA's actions to implement the espoused theory, it was revealed that the governing variables include developing a common security program for the state, establish base practices in all agencies, and blanket compliance with the state security policy. The action strategies formed to satisfy the governing variables indicate a clear bifurcation of roles in terms of development and implementation between the ITA and agencies. The security department at ITA took on the responsibility of developing the security policy, standard and guidelines. However, it was the responsibility of agencies to implement the security program in their respective organizations. This has inherent implication that the ITA does not have responsibility to assist agencies in implementing the program. Such a strategy does make sense but we have to understand the underlying contextual changes in the state.

The reality was that most of the agencies had lost their technical expertise to the ITA as part of a statewide consolidation of information technology. The ITA was made

in charge of the IT infrastructure for the state and provided reasonable argument that the supporting technical human resources should move to the ITA as well. With the security initiative, the expectation was that the ITA would be helping agencies to implement required security initiatives. However, this did not happen. Agencies got frustrated with the ITA as it had procured all the technical human expertise from agencies and now expected agencies to somehow implement the program on their own. To worsen the situation, agencies were in fact paying the ITA an exorbitant sum of money for IT resources and services. Few of these services, like intrusion detection and prevention, were non-existent for long period. The situation was so bad that even security department members would openly acknowledge that all agencies hated them. It would be fair to say that the security group was not able to achieve the intended outcome. In light of negative consequences, which included widespread frustration and discontentment, the security department decided to change the action strategy.

A new CISO was appointed to lead security operations at the ITA. As part of the new action strategy, the role of security department was changed to that of governance. The group slowly moved away from technical security responsibilities. As a result, two in-house technical security experts were let go off. The CISO placed emphasis on development of an information assurance program. At the same time, all agencies were required to get compliant with the state security policy within a year. Subsequently, the audit department was merged with the security group. The current CISO was in fact the head of audit department before taking on additional responsibility of the security officer. As a result of merger, the title of CISO was changed to Chief Information

Security and Audit Officer. The role of compliance and governance were made prominent at the security department as part of the new action strategy. However, agencies remained skeptical with the new efforts. In fact, agencies perceived new action strategies on part of the ITA as an emergence of policing role. The merger of the security department with the audit department was seen as a message that security was considered to be an audit function by the ITA. Agencies resented the fact that the ITA security department had evolved to don the mantle of state police with respect to security operations. It is important to emphasize that agencies had issues with the merger of auditing and security functions. Based on interviews at DOT, it seems that agencies might have been receptive and understanding about the governance role for the ITA. Towards the end of the research period, agencies had even more reasons to hate the ITA security department.

The problem remained that agencies were not getting any effective help to implement the security policy. In particular, agencies of medium and small scope felt they have been left on their own. The security department does claim that they are indeed helping agencies as much as possible. However, observations by the researcher indicate that the approach has been more hands-off. The help extended is more in terms of providing high-level guidance as to what documents or things are required for compliance purposes. There are no expert teams available. There is absolute lack of skilled members whom are proficient in the discipline of information systems security by virtue of education or work experience.

Employees have been hired depending upon convenience of availability rather than possessing necessary skills. The security management team argues that skilled people are not available. As a result, the approach has been to appoint people who are willing and then train them on the job. Many security department members have actually taken their security certifications after they had started working on the new position. Even management team of the security department does not have significant understanding about information systems security issues. The management team has mostly audit background and therefore seen to approach security function from the perspective of audit mindset. The criticism is not about the intelligence or capability of these members but the apparent lack of security skills. It comes rather surprising that such significant managerial positions are not occupied by individuals with reasonable skill sets in the field of information systems security. This may also be considered as the reality of government functioning and a criticism of the same.

The reality is that because of various reasons or failings on part of the ITA security department, numerous agencies have been left stranded to implement the security policy without adequate resources at their disposal. Needless to say, there is a general mistrust and frustration when it comes to deal with the ITA in general and its security department in particular. This problem would continue to persist even if alternative action strategies are developed to satisfy the existing governing variables. At this stage, it becomes imperative for the security group at ITA to address the prevalent double loop issues. The appropriate solution would be to re-evaluate existent governing variables and bring them into alignment with the espoused theory. Once the espoused

theory and the governing variables of theory-in-use are congruent, action strategies may be developed to satisfy the newly developed governing variables. Such actions would help achieve outcomes as intended by the security group. Nevertheless, there would be few unintended consequences associated with any action that would have to be taken into account. Such is the nature of the business world.

7.4 Strategic Information Systems Security Initiatives at DOT

The following discussion is based on the empirical evidence presented in chapter 6. In this section, the information systems security initiatives at DOT are the focus of analysis. At DOT, the responsibility to develop and subsequently implement information systems security program was given to the Information Technology Division.

7.4.1 First-level findings

The security initiatives at DOT were formulated in response to the need to abide by the state legislation on information systems security while satisfying business objectives.

Organizational restructuring

The events unfolding at DOT influenced by circumstances of both internal and external context led to restructuring of the organization. Aftermath of internal power feud and the necessity to comply with security related state legislation created a

favorable situation for the IT division to get information systems security operations under its control. Once the information security operations were moved, the CIO took on the additional responsibility of the CISO as well. This enabled adequate allocation of resources for the development and subsequent implementation of security initiatives within the DOT. The CIO deputed his trusted project manager to head the security operations as the Deputy CISO. Such a move was to ensure that required compliance with state legislation is met by the specified deadline. This would also help in legitimizing the move of security operations under the IT division.

Adopt the state security policy

The IT division took on the responsibility to develop the security program as specific to context of the DOT. The security group within the IT division decided to adopt the state security policy and standard in its entirety. To address organizational requirements, a security manual was developed along the lines of the state security policy but the procedures outlined in the document were configured as per internal business requirements. The security manual detailed various security procedures required to ensure secure information related operations within the DOT.

The security group was careful to properly communicate security objectives in the program manual exactly as captured in the adopted security policy. This helped in selling the authority as coming directly from the state government. It also protected security group. In case of any untoward security incident, the security team can argue

that they did not write the security policy but rather were simply adopting and implementing the state recommended policy. As such, the group may not be held directly responsible for the weak policy. Since the security policy was actually developed by the state technology agency, it is expected that the state would indeed protect the DOT from any stringent punitive actions in case of an untoward security event.

Executive leadership

In order to control organizational environment, strong management support was considered to be critical by the security group for success with the program. To emphasize support, the CEO sent out a memorandum addressed to all heads of divisions and districts at DOT emphasizing his commitment to enforce the security program. Strong leadership was necessary for the security group to overcome organizational hurdles while promulgating the security program within the DOT.

Ensure compliance with policy

Another goal defined by the security group was to ensure that all organizational members had read the adopted information systems security policy. In order to demonstrate compliance, all members had to complete an online security training program at the end of which each individual was issued a certificate of completion. This certification of compliance was to be obtained each year by all organizational members. The attainment of ninety percent compliance in terms of online certification from users

by June 2007 was considered to be an effort to show figures as proof towards success with security initiatives within the DOT.

The failure to attain an online certification was perceived as a message from a user that she does not agree to abide by the security policy. For such users, the CISO decided to turn off account access until user demonstrated obedience to authority. Such an action may also be seen as protecting oneself as the certificate of compliance essentially indicates that a specific user has read and agrees to abide by the tenets of the security policy. Hence, each user may be held accountable for her information related actions.

Implement some form of the security program

The state required all agencies to get compliant with the state security policy within a year. To abide by this directive, emphasis of the security group was to implement some form of the security program in all divisions and districts of the DOT. This would allow the DOT security group to argue that the intent of getting compliant with the state security policy is there even though they might not have been able to get cent percent compliant. The group in fact decided to develop formal records depicting proposed implementation plans of the security program across the organization. In terms of executing the security program, it became essential to convince and build relationships with the heads of various divisions and districts at DOT. Towards this end, a position of information security coordinator (ISC) was created in each division and

district. This was done to support the heads of divisions and districts in handling their responsibility for implementing the security program in their respective domains.

The new ISC position was used to sanction security aspects and also as a communication source for the respective division or district. This position was funded by the IT division to help in developing a shared vision about security related goals. Further, the CISO gave up the facility of control over these positions to the division and district heads in order to avoid any untoward power conflicts. At the same time, the security group also focused on the maintenance and upkeep of the security program. To take the security program to a level of maturity, the group concentrated on developing skilled process, having skilled people and skilled manager at the helm of security efforts.

Pressure to overcome skepticism about security program

Although skeptical about the effectiveness of state information systems security policy, the security group members at DOT seem to consider it as one that would get the job done. The security group realized that state legislation requires them to get compliant with the state security policy at the minimum. For expediency purposes, the CISO had decided to adopt the state policy in its entirety and directed the group not to question the policy but first implement it across the organization in some form.

The security group created awareness of the security program among organizational members. Security related workshops were conducted for the officers of responsibility from each division. A website was created for incident reporting, awareness training, cyber tips, and making available the security policy and manual.

This website was allotted a prominent position on the main organizational portal. In addition, each employee was required to undergo the online security training and obtain certification of compliance each year.

Approach the security program as just another project

The CISO decided to approach establishment of information system security program as just another project. The first phase was directed towards development of the security program, while second phase was focused to implement the security program within the DOT. The CISO decided to adopt the state security policy in its entirety thus scaling down the time component of the project significantly.

The emphasis of security group has been to implement the security program as much as possible by the compliance deadline. For areas where security program could not be implemented by the deadline, the group was directed to develop a concrete direction plan for implementation. It was hoped that in case of an audit the group might be able to make the case that plans are in fact in-place to address uncovered areas. The subtle implication is to convey the impression that efforts are underway to ensure that the security program is instituted within organization as required by the policy.

7.4.2. Second-level findings

In this section, the second-level findings pertaining to the information systems security efforts at DOT are presented and explained.

Security program as constitution of the meanings and intentions of actors

An action is to achieve certain consequences. The actions undertaken at DOT were to make the organization more secure and also comply with state information security requirements. Any action may be considered as designed by an actor (Argyris and Schon, 1974). As such, we may assume that an action is constituted by the meanings and intentions of actors. In this manner, the security initiatives at DOT can be understood through theory of action. As mentioned in section 7.3, the theory that an actor claims to follow is referred to as espoused theory, while the theory-in-use is the theory that actors actually use and can be inferred from their actions.

Let us first identify the theory-in-use for information systems security initiatives at DOT. The theory-in-use involves three main components in the model – governing variables, action strategies, and consequences. Governing variables are the values that actors seek to satisfy (Argyris Putnam, and Smith, 1985). For the DOT, the governing variables for security implementation was to adopt the state security policy in entirety, implement some form of security program across the organization, ensure compliance with security policy, exhibit confidence in the security program, and approach security program as a project to make sense of the complex subject. Previous section discussed the actions that were followed by the security group at DOT to support the four governing variables. Action strategies are sequence of moves used by actors to achieve desired results that will satisfy governing variables (Argyris, Putnam, and Smith, 1985). The strategies of action at DOT are summarized in table 7.2.

Table 7.2: Unilateral control model for security implementation at DOT

Governing variables	Governing variables for security implementation	Security implementation strategies of action
Define goals and try to achieve them	Adopt the state security policy in its entirety; develop the security manual for internal operations.	Restructure the organization; allocate adequate resources; depute skilled manager to head the security operations; develop the security program; ensure strong management leadership.
Maximize winning and minimizing losing	Ensure compliance with security policy; implement some form of security program in all divisions and districts.	All organizational members to read the security policy; create information security coordinator position in all divisions and districts; emphasize maintenance and upkeep of the security program; focus on skilled manager, people and process.
Minimize generating or expressing negative feelings	Exhibit confidence in the effectiveness of the security program.	Create awareness of the security program; conduct security workshops; attain a prominent position for security website; impart online security training and certification of compliance; properly communicate the security objectives; sell the authority as coming directly from the state legislation.
Be rational	Approach security program as just another project.	Implement the security program as much as possible by the compliance deadline; convey the impression that efforts are underway.

Interpreting intended and unintended consequences for single-loop learning

An action leading to unintended results may be undesirable for actors. In such a case, an actor would generally develop a new action strategy in order to achieve the desired result. Such an action enables single loop learning as the new action has been developed within the confines of existing governing variables. Since all consequences eventually feed back into action strategies and governing variables, it becomes important to understand the consequences of actions at DOT in order to effect single loop learning.

Concern for self and manipulative tendencies of the management

The executive officers at DOT were defensive about empowering the existent Operations Security division or restructuring it as an independent department reporting directly to the CEO. After security operations were reallocated to the IT division, security was still not given an independent status and was placed under the governance group. Such restructuring was undertaken despite questions raised by stakeholders, like IT auditors, about conflict of interest. The IT division wanted to control security policy development in order to continue its current practices of systems development. The restructuring may also be attributed to the department's apparent fear of being vulnerable to the requirements of security policy in terms of secure IT development. The CIO seemed confident in his department members ability to do a good job on self-policing. That is, department members were considered to be competitive enough to develop required security policies so as to ensure secure development of information systems at DOT.

In order not to fail with state compliance, the IT division developed an efficient strategy to adopt the state security policy. Such an action, void of any consideration to the context and business requirements of DOT, indicates inconsistency with the known security practices. However, such a superficial compliance with the state policy demonstrates competitive nature of the department management team indicated by their concern to show the results. The IT division got control of security operations despite some resistive concerns and, in case compliance is not achieved by the deadline, such voices would be redeemed. As such, the management seems to be interested in

achieving a superficial compliance rather than developing an appropriate security program based upon business needs of the DOT.

Defensive interactions of the security group

In order to minimize the chances of failure during implementation phase, the security group created ISC positions in each division and district. These positions were also funded by the IT division, which further implicitly established the dependence of divisions and districts upon the security group. The control of the newly formed ISC positions was given over to the respective division and district heads. This actually led to unintended consequences for the security group. In some instances, the ISCs were hired without any security background or qualification to perform non-security related tasks, such as financial reporting. During the implementation phase, ISCs were pushed by the security group to take responsibility for implementing security program at their respective positions. The security group was surprised to learn that individuals at ISC positions were not hired to perform security tasks and such tasks were actually creating additional work for the position holders.

Defensive norms

The security group has a general mistrust with other departments both in terms of intent and capability. This impacts subsequent dealings with divisions and districts within the organization. Rather than expect voluntary compliance, the organizational members were forced to read the security policy else face the threat of terminating

account access. The online certification was simply a mean to protect oneself in case of any adverse incident with suspected employee involvement. Further, a number like ten percent of the accounts terminated due to non-compliance indicates that efforts are underway and some positive results have actually been achieved. This is a demonstration of the defensive norm of rivalry whereby the IT division wants to show that they can do a better job than the Operations Security division, previous guardians of information security within the DOT.

The management of IT group decided not to take risk by exposure to new weaknesses as a result of developing a new security policy. Hence, management ended up simply adopting the expected minimum compliance requirements. The external commitment is considered to be another defensive norm. The commitment of security group to adopt the security policy developed by an external state authority as better policy is indicative of such a norm. The decision to implement what is outlined in the security policy shows emphasis of the CISO on diplomacy. The underlying aim was to shift the responsibility for any prospective security weakness to the sponsors of state security policy.

Lack of internal commitment for best security practices

There is little freedom of choice in developing security controls and procedures as these are bound by the state security policy. These controls have to be within the range of advocated policy. That is, the security controls and procedures are restricted to the tenets of the adopted policy. As a result, there is little commitment to institute best

security practices. The process of implementing the security program becomes merely an exercise to check few boxes for compliance purposes. The security group members end up not taking any risks and play a safe game. Subsequently, users are also not committed towards cumbersome security practices.

For theory-in-use model, all consequences have an impact on action strategy and overall governing variables. The underlying behavioral strategy for this model (theory-in-use) is unilateral control over others. This was evident at DOT. The establishing of security initiatives was potentially critical situation for the DOT and organizational members were most oriented to control others and protect themselves.

Explicating the espoused theory of information systems security caretakers

In this section, we would discuss the espoused theory of the security group at DOT. An actor is generally only aware of the espoused theory, as this is the one she claims to follow. The espoused theory gains significance as any mismatch with the theory-in-use would lead to undesired results.

At DOT, the CISO encouraged participation of all organizational members for the development of information systems security program. During interviews, the management team for security efforts, including the CISO, the Deputy CISO, and the manager of governance group emphasized how they have listened to various stakeholders and sought their feedback for developing an effective security program. Managers from different departments of the IT division participated during developmental meetings. The versions of security manual documents would be passed

onto these managers for their comments. Participation of stakeholders in defining the security program was one of the goals articulated by the security team.

The second governing variable for espoused theory is that everyone wins and no one loses. At DOT, the push by state legislation to get all organizations compliant with the state security policy was indeed seen from such point of view. The management at DOT considered that getting compliant with a security policy by successfully implementing it would in fact help the entire organization by rendering its business operations more secure. A secure information environment was seen as beneficial. At the same time, the DOT would also be able to observe the requirement as necessitated by the legislation. In the process, it would be able to generate goodwill among legislators by presenting a positive secure image.

At various stages of development and implementation of the security program, organizational members working on the security team or as users were requested to freely express their concerns regarding the program. Members were asked to provide comments and feedback on various components and aspects of the security program including the security manual and the training program. Free and proper expression of feeling is the third governing variable for an espoused theory. In fact, user feedback was considered critical for success with the program. These users were actually at different levels of organizational structure. Initial emphasis of security team was to focus on the executives that would be considered as responsible for information system security in their specific domains.

The final value generally sought to be satisfied is to suppress the cognitive intellectual aspects of action. The security group at DOT decided to adopt the state security policy as required by legislation. The group decided not to change any element of the security policy. But rather, a security manual was developed that were to reconfigure the policy requirements as applicable to DOT's operational environment. Such a move prevented stakeholders from questioning the legitimacy of specific action or suggestion by the security group.

Double loop learning

An action is performed in order to attain desired consequence. However, in certain cases actions undertaken fail to provide the necessary outcome. In such a case, we would generally pursue a new action in order to address the apparent error. This enables single-loop learning. Argyris Putnam, and Smith (1985) explain that double loop learning would require an actor to change the existing governing variables in order to get the desired outcome. The actor would have to bring the new theory-in-use in congruence with the espoused theory for effective results. Any mismatch between the espoused theory and theory-in-use essentially has double loop implications for the situation (Argyris Putnam, and Smith, 1985).

As per the espoused theory, the DOT has adopted the state security policy and considers its implementation as actually a good thing for the agency. However, the theory-in-use indicates development of a security manual for security operations at DOT. The apparent incongruence between the espoused theory and theory-in-use

creates a gap that could be problematic for the DOT as an organization. As discussed previously, the state security policy has potential faults. If security manual were based upon the state security policy, inherent faults in the policy would creep in and impact IT operations. The interviews with departmental members indicate that the DOT already had an existent security program. With the advent of the state security policy, department decided to convert the existing security policy into a security manual and made structural changes to the manual so as to give an appearance that manual is indeed based on the state security policy. This creates a serious problem as inherent argument or logic of the state policy is nullified by actually adopting pre-existing security policy that was converted to security manual. The inherent logic of the policy is different than that of the manual and as such poses problems for coherence in the security posture. This in fact is camouflaging of the potential issues.

In terms of implementation, the espoused theory at DOT was to ensure compliance by all organizational members. However, a careful look at the theory-in-use indicates superficial compliance by all members. The security department emphasized the need for security training for all employees. As part of the online training, each organizational member was expected to read the security policy and answer few questions to earn completion certificate. The security management team used online certification as a stick to ensure that all members had read the policy so as to be able to measure compliance. Such a number was touted to be around ninety percent compliance. In actual, the online training program was considered a joke by technical (IT) members of the organization.

For organizational members, the training was informative in beginning but soon lost appeal and appeared to be redundant with stale information. Further, members could simply go back and forth to answer the questions. Almost all members interviewed informed that they did not even had to read the security policy and could simply complete questionnaire in five to ten minutes as answers could generally be known with few tricks. As such, what has happened here is superficial belief or comfort in compliance numbers. In fact, user education about information systems security did not really happen. The high compliance number would create a false sense of confidence in the security program so established. This issue certainly raises further questions about the real state of security at DOT. It might be the case that effective security controls are very well in place. This might raise a question as to why then management wants to lull itself into false pretence. The answer might be the relative comfort in numbers and the need to measure every task so as to judge it as successful or not. This poses an interesting question whether security can really be measured and quantified.

7.5 Discussion

The theory of action, as proposed by Argyris & Schon (1974), aims to help organizational members initiate actions to change the business environment in congruence with the values imbibed in their espoused theories. In order to attain the normative perspective of an espoused theory, we may design actions consistent with the Normative Model II as proposed by Argyris and Schon (1974). The use of such a model

would most likely enhance the likelihood of double loop learning and increase the effectiveness over time (Argyris Putnam, and Smith, 1985). For the normative model, the governing variables include valid information, free and informed choice, and internal commitment. Based on the two case studies, the normative model II as interpreted for information systems security is presented in table 7.3.

Table 7.3: Normative model for information systems security

Governing variable	Information Systems Security strategy	Expected consequences for security initiative
Valid information	Design an organizational environment conducive to collaboration among stakeholders. Facilitate stakeholders to create a contextually driven security initiative.	Consistent application of organizational security values attaining contextually authentic security initiative.
Free and informed choice	Security initiative jointly controlled by interested parties.	Effective security related group dynamics enabling double loop implications.
Internal commitment	Sustenance of security initiative through constant monitoring of its implementation. Minimize inconsistency between security requirements and security controls and procedures. Joint cooperation across different levels of organizational structure. Bridge gaps in departmental interests for a secure business environment.	Establishment of trust in security operations leading to security conformity.

The implication of ‘valid information’ as a first governing variable is to ensure that information is in congruence with the context of an organization. This would allow correct assessment of the operating environment in terms of information system security needs of the organization. Contextually driven information would assist organizational members in making appropriate decisions conducive to secure business operations. The strategy to design an associated action would require sharing control with members having competence and stakeholders involved in the development, as well as,

implementation phases. The information systems security strategy would involve designing an organizational environment conducive or sympathetic to collaboration among stakeholders. The emphasis is on facilitating situation such that members of the security group are able to create a contextually driven security initiative. This would allow consistent application of organizational security values attaining contextually authentic security program.

The next governing variable in the model is free and informed choice. In terms of information systems security, this governing variable necessitates an appropriate selection of the security program as necessary to achieve secure organizational environment. It is imperative to understand the requirements of an organization and then make judicious decision on an appropriate security framework or standard to be adopted. At the same time, an organization should not impose restrictions on its stakeholders to make a selection among specified set of standards. The security group should be provided flexibility to identify a security framework that is appropriate given the contextual environment. The security policy may then be based on the identified framework and would inherit the latter's inherent logic. The security program can then flow from the structure of the policy. The information systems security strategy to be followed should allow conflicting viewpoints to be externalized such that underlying theories can be tested openly. Such a strategy would require all tasks formed towards the security initiative to be jointly controlled by interested parties. The pursuance of this security strategy would allow effective security related group dynamics enabling double loop learning.

The final governing variable of internal commitment emphasizes the need for processual commitment to the security initiative. An internal commitment to the choice indicates that appropriate action need to be taken by the management team to ensure that the security initiative is successfully adhered to. This essentially means that necessary processes need to be established within an organization in order to implement the security initiative. At the same time, establishment of such procedures and controls necessitate strong management leadership in the first place. In addition, the sustenance of security initiative through constant monitoring of the implementation of security program is imperative in order to attain the desired results.

The information systems security strategy to be followed should allow interruption of self-sealing processes. This would also lead to discussions on problematic issues and underlying assumptions might be re-evaluated. Any inconsistencies between security requirements and advocated security controls and procedures during implementation process have to be minimized through joint efforts of stakeholders. In essence, the need is for joint cooperation across different levels of organizational structure that is oriented towards a secure vision for everyone's benefit. It is imperative to design strategy that helps bridge gaps over departmental interests so as to create a secure environment for the organization. The security actions outlined as part of the security strategy would establish trust in security operations of the organization thereby enhancing security conformity.

Bringing theories-in-use in coherence with the espoused theory of the security group would indeed help effecting security change in an organization. The dissertation

began with an observation in chapter 1 that there have been problems in industry with lack of success with security initiatives. The reason we have security failures in organizations is because there is too much emphasis on deliberate rational planning leading to rigidity rather than striving to ensure flexibility as exhibited in strategic initiatives of emergent nature. Mintzberg (1987) considers the fundamental dilemma of strategy formation to be the need to reconcile the forces for stability and for change. The author proposes quantum theory of strategic change. As argued by Mintzberg (1987), organizations adopt two distinctly different modes of behavior at different times. Generally, organizations pursue a given strategic orientation. Incremental changes keep occurring within the confines of that orientation. However, the organization's strategic orientation moves out of sync with its environment as the business world keeps changing.

Long period of evolutionary change is suddenly punctuated by a brief bout of revolutionary turmoil in which organization quickly alters many of its established patterns (Mintzberg, 1987).

The organization tries to leap to a new stability quickly to reestablish an integrated posture. That is, strategic reorientation happens in brief, quantum leaps.

Based on the quantum theory of strategic change, we may infer that any strategic information systems security initiative needs to happen in brief, quantum leap. During such reorientation, theory-in-use is brought in alignment with the espoused theory. For quantum security change to happen, an initiative should imbibe strategies outlined in table 7.3. This adapted theory does seem to hold for the two case studies discussed in this research, the ITA and the DOT. In case of the DOT, the security related change

indeed occurred in brief yet quantum leap. The organizational restructuring, development of the security program and its subsequent implementation took place in less than a year. The security change process has been considerably smooth relative to other change efforts in the organization. The security group was able to achieve its objective of getting compliant with the state security policy before the state specified deadline.

The case of ITA is in direct contrast to security efforts at DOT. For the ITA, the security related change initiatives have been going on since 2003 with the passage of state legislation. The initial effort to achieve information systems security goals for the state has been abysmal. The efforts of security group ended up creating a confused and frustrating situation for agencies in the state. The appointment of a new CISO in 2005 and subsequent renewed emphasis gave security initiative a new push. However, the new security related changes were not without problems as has been discussed earlier. By end of 2007, the security initiatives undertaken by the security group at ITA could be deemed unsuccessful in attaining its main objective of establishing a common information system security program in the state. The CISO had to extend the deadline for compliance with the state security policy in the wake of predominant failure of number of government agencies to respect the deadline. The security change has been going on far too long.

Based on this research, a theory to help explain the information systems security related change in an organization is put forward. The theory of quantum strategic security change (QSS) states that strategic information systems security initiatives

would be successful in an organization if developed and implemented in a brief yet quantum leap adopting an emergent security strategy in congruence with organizational security values, adhering with security cultural continuity, establishing effective security governance structure, ensuring security related knowledgeability, and commitment to security processes. To develop the strategic security initiative effectively, we need to ensure that the initiative is harmonious with the continuity of organizational culture. The security culture needs to ensure continuity of existing opportunity structures and not frustrate the expectations of organizational members. The development of security cultural resources like security policy and standards would obscure the quest for power and establish dominance that would allow propagating the secure view of the social world.

The successful implementation of the security initiative is dependent upon the organizational security structure and knowledgeability of agents in terms of security related self-identity and organizational identity. At the same time, adequate attention need also be paid to global security catalysts establishing trust relations between security agents, and institutional reflexivity for security effective practices. The strategic security initiative would be effective in bringing about security related change in an organization when the actual action strategies developed to secure the information environment are in congruence with the espoused security values of an organization. Such actions to institute security initiative need to be based on valid information, selected by informed choice, and supported by internal commitment of an organization.

7.6 Conclusion

This chapter has described information systems security initiatives at the ITA and the DOT from an action perspective. Such an approach was argued to be conducive in understanding different strategies of action needed to support an information systems security initiative in an organizational context. The analysis in this chapter has evidently shown the effectiveness of Argyris and Schon's (1974) theory of action to explain the intricate relationship between content and process, along with context of an organizational security change. Based on the emergent issues from the two case studies, the theory of quantum strategic security change has been developed to help explain the success or failure of a strategic information system security initiative. The proposed theory is intended to help the executive officers of an organization in effecting a successful information systems security change in modern organizations.

CHAPTER 8

Conclusion

8.1 Recapitulating the Doctrine

This dissertation has explored issues surrounding strategic information systems security initiatives. Strategic information systems security has been defined as a plan or pattern of actions to attain viability and effectiveness of an organization by securing information handling activities in the light of changing critical environment. The purpose of this section is to summarize key ideas and identify the contributions of this dissertation. In this section, we first present the nature of strategic information systems security, followed by shaping such security initiatives in organizations. Finally, the issue of technology governance is discussed.

8.1.1 The nature of strategic information systems security

Information systems security researchers and practitioners have tried to minimize the security gap in organizations through technical solutions and changes to organizational practices and structures. There have been efforts to consolidate different security functions. Also, prescriptive rationalistic planning has been imbibed by organizations to develop the security program. Although good in intention, the explicit

dependence upon technical solutions and rationalistic planning only takes into account the anticipated changes in the business environment. In contrast, this research has considered strategic information systems security to be emergent in nature conceptualized as a plan or pattern of actions. It has related the development and institutionalization of strategic information systems security to the contextual aspects of an organization. The implicit argument is concerned with aligning the interconnections between the security content and processual security with the contextual conditions of an organization.

The argument of this dissertation has broadened the scope of information systems security discipline. The need for strategic approach to security efforts has been emphasized in order to overcome the security failures. It has been argued that a plan or pattern of security actions needs to be undertaken with a proper understanding of the content, processes and context of an organization. The key concern has been considering the impact of interaction between content, processes and context of an organization. It is important to align the linkages between these key components of a strategic security initiative.

In developing the security program, the content of such a program should be considered with respect to contextual intricacies. A security initiative would be successfully instituted in an organization if it indeed were harmonious with the cultural continuity of an organization rather than significantly changing the existing opportunity and constraint structures leading to frustrating the expectations of actors. The security culture may also be used as a tool for propagating the secure view of the social world.

At the same time, we cannot divorce such development from the interactions between processes and context. For organizational transformation, we need to address the organizational structure and knowledgeability of agents in perceiving organizational identity in terms of security. At the same time, it is pertinent for organizations to consider the modernity concepts of self-identity and global security catalysts such as disembedding mechanisms and institutional reflexivity.

The reason for failures with security initiatives has been argued to be rigidity arising from emphasis on deliberate rational planning. The problem is to enact the content through various practices within a specific context. It has been suggested that strategic information systems security initiatives would be successful in an organization if developed and implemented in a brief yet quantum leap adopting an emergent security strategy in congruence with organizational security values, adhering with security cultural continuity, establishing effective security governance structure, ensuring security related knowledgeability, and commitment to security processes.

8.1.2 Shaping the strategic information systems security initiatives

Information systems security research needs to mature from formistic and mechanistic tendencies and ground itself in contextualist paradigm. The complexity of information systems security has been traced by defining the set of beliefs and assumptions about the nature of social reality. We need to critically address philosophical questions in the context of information systems security. Different ontological and epistemological assumptions would lead to different approaches to

security. The critique of current approaches lays foundation for contextualist perspective in dealing with the security issues.

The dominant security research theme has been to find the factors or components that would impact overall organizational security. The mechanistic tendencies in information systems security research have also been noted which informs us about the casual connections in the nature of information systems security. The universal structure of information systems security is analytically investigated to identify the components in order to explain its true nature.

The increasing complexity of business environment in which organizational security has to be operationalized necessitates the need to understand the context in a dynamic manner. In order to improve the security posture of an organization it is imperative to realize, intuit, and get the quality of an event of interest, which involves an act in and with its setting (Pepper, 1970). At the same time, it is also important to understand the constituent, as well as, processual models for implementation of a successful information systems security program. However, it is imperative to be eclectic rather than study the security problem in a static manner.

8.1.3. The issue of technology governance

This research has emphasized the importance of contextualist perspective while strategizing about information systems security posture of an organization. This leads to an important issue that of technology governance. There has been an increasing concern for information privacy amid prevalent problem of security incidents. The government's

response to such concerns of the citizens has been to simply fall back on the tested doctrine of standardization. That is, the solution has been conceived as to establish standard security practices within an industry. For instance, organizations operating in the medical industry have to deal with Health Insurance Portability and Accountability Act of 1996 (HIPPA). Both federal and state governments have introduced various regulatory artifacts to ensure secure IT environment.

Organizations now have to operate in an increasingly federated environment. Quite a few organizations are basically reacting to the compliance requirements set forth by the government. The organizations are expected to abide by the tenets of these regulatory artifacts. The legislations that provide generic guidance or stipulations, such as mandatory security policy in all organizations, can actually be helpful. However, the problem arises when legislation provides directive to a government entity to develop a security policy that need to be complied by all organizations in an industry. The concern is with the prescriptive nature of the security artifact and assumption that one shoe fits all. In order to have sweeping coverage, such policies generally ignore the contextual aspects of an organization

In reality, many organizations find themselves under purvey of more than one set of regulations. For instance, publicly traded financial institutions have to comply with the requirements of both Gramm-Leach-Bliley Act (GLBA) and Sarbanes-Oxley of 2002 (SOX). This indeed can be a very daunting task. In order to check for compliance, government then have to rely upon auditors for evaluating the state of security in organizations in regulated industry sectors. The government, however, is not

to be blamed especially in the wake of corporate scandals and increased interest in corporate ethics. The march of the auditors is generally perceived negatively by organizational members and is often reminiscent of policing. This has nevertheless contributed positively to the economy with an ever-growing cottage industry of IT auditing.

In view of growing federated requirements, organizations might be lulled into lethargic behavior where they may consider complying with mandated regulations only. This would create false sense of security as the very regulatory artifact may be based upon (and in fact preaching) limited view of security. Such an approach might be an effective way to deal with bureaucrats but results can be endemic. These situations call for effective technology governance, specifically with respect to security issues. IT management faces the dilemma of trying to comply with all government requirements and yet remain effective from a security point of view. The senior executives have to plow through plethora of standards and frameworks and decide upon an appropriate direction. However, only so much can be done. The main objective of an organization is to either maximize profits (for a corporate firm) or maximize service provided to customers (for a government agency). The organization does not exist simply to implement all the standards or regulations prescribed by the world.

Organizations need to focus on strategic information systems security initiatives in this fast paced business environment with continuous regulatory compliance requirements. The need is for prudent technology governance. Such leadership should not be distracted by technology fads but rather focus upon sound security principles. It

is imperative for technology leaders to realize the enabling role of information systems security. Strategic information systems security would allow organizations to be proactive and prepared for unanticipated business changes. The intent is to develop security content and subsequent security processes in coherence with contextual aspects of the organization.

8.1.4. Summary of contributions of this research

This section summarizes the main contributions of this research.

Broadening information systems security approach: The emphasis of information systems security literature has been on deliberate rational planning for security endeavors. Such prescriptive efforts are problematic because the attention is given only to the anticipated conditions of future. It is essential to also account for the unanticipated conditions, which render further complexity to business environment. This research has in fact broadened the approach to information systems security problem by tackling it from a proactive or an emergent perspective. This research views strategic information systems security as a plan or pattern of actions to attain viability and effectiveness of an organization by securing information handling activities in the light of changing critical environment.

Theory building: One of the main contributions of this research is building theory in information systems security discipline. It has provided a thorough description of the issues and concerns in transforming an organization for strategic security change

to avoid the possibility of security failure. The contribution of this dissertation is to bring together research in strategic management, information systems and information systems security, and also introduce a contextualist approach to development and institutionalization of strategic information systems security initiatives.

Contextualist strategic security: This research has argued that to solve the problem of information systems security failures, we need to understand the contextual perspective of an organization. The theory of contextualist strategic change has been used to identify the areas of concern that would have an implication for security posture of an organization. This research also identified an oversight in the application of this theory in information systems literature. Consequently, the need to focus on inter-connections between content, context and processes has been emphasized.

Understanding security culture: This research has used cultural perspective to study information systems security initiatives. The concept of security culture has been of intrigue to security discipline and yet limited research has been undertaken to unravel this concept. This research has introduced a sociological approach (Pierre Bourdieu's cultural theory to study practices) to understand the role of security culture in shaping the strategic security initiatives. The cultural approach provides a rich interpretation of security practices and helps create opportune organizational environment sympathetic to instituting strategic security initiatives.

Organizational security transformation: In order to effect a successful security change, this research has developed a model incorporating the security governance structure, knowledgeability of agents in terms of security and global

security catalysts. This model is grounded in the structuration theory and the theory of social transformation. The application of this model helps in an effective transformation of an organization embarking upon strategic security initiatives. The components of the model would help a practitioner in identifying specific security implications as applicable to modern organization. Although comprehensive, the model does not claim to address every granular element of organizational life.

Principles for shaping the strategic information systems security initiatives:

Based on the empirical evidence from two case studies, this research has established a set of principles for shaping the strategic information systems security initiatives in an organization. These principles are intended to attain the normative perspective of initiating strategic security change. A proper consideration of these principles would help develop effective practices in creating a secure organizational environment. It has been argued that the reason for security failures has been lack of flexibility (of emergent nature) in security efforts. Such failure may be overcome by initiating strategic information systems security initiatives in a brief, quantum leap to achieve the desired security posture. The organization need to adopt an emergent security strategy in congruence with organizational security values, adhere with security cultural continuity, establish effective security governance structure, ensure security related knowledgeability, and commit to security processes.

The findings from this research are intended to be valuable to the community of researchers and practitioners engaged in the study of confluence between information systems security and organizations. It provides insight to the phenomenon of security

change and helps us understand some of the critical issues in preventing security failures. This research is mere beginnings and provides a basis on which further work can be built upon.

8.2 Limitations and Future Research Directions

This section identifies few limitations of this dissertation and outlines future research related to the development and institutionalization of strategic information systems security initiatives. These are discussed in terms of theoretical concerns and methodological issues.

8.2.1. Theoretical concerns

Dhillon (1995) presents a model for classifying theories and uses it to provide future research directions (figure 8.1). The classification model has micro-macro distinction concerned with level of analysis as one dimension. Here, micro refers to the local form of social organization, while macro refers to large-scale social system. The second dimension of model is the substantive-formal distinction concerned with generality of categories with respect to cases. The formal categories are restrictive as compared to substantive ones. This model provides a four-fold classification of theories.

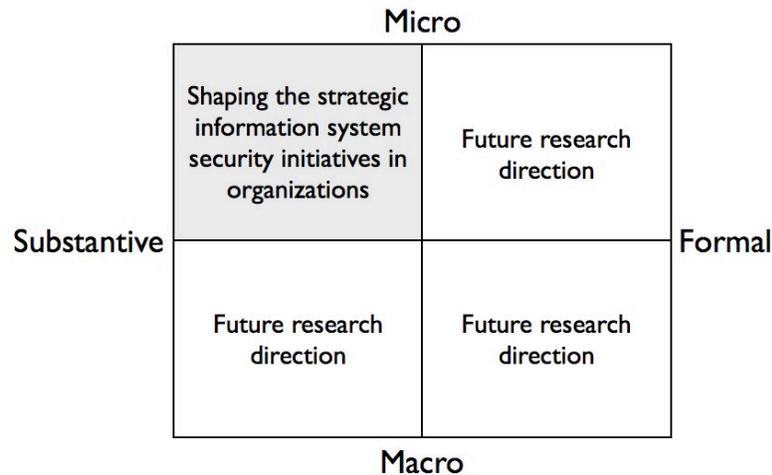


Figure 8.1: Future research directions (Adapted from Dhillon, 1995)

Macro-formal theories are concerned with the structure, functioning and development of societies. On the other hand, macro-substantive theories involve studies pertaining to a particular industry. For micro level of analysis, the theories concerned with local forms of social organization are categorized as micro-formal theories. On contrary, the focus of micro-substantive theories is on particular types of organizations or situations.

Based on the model, this research falls in the micro-substantive category. This is because the approach of this dissertation has been to consider contextualist aspects of organizations for instituting strategic information systems security initiatives. This research has focused on a particular type of organizations – government organizations operating in a federated environment. This may be considered as a limitation of this

dissertation. As such, future research stream should validate the findings in different organizational and industry settings. Such directions could focus on rest of the theoretical categories. For instance, research findings from this dissertation can be used in other public sector organizations to develop a macro-substantive theory.

Alternatively, we may be ambitious to develop a macro-formal theory. Such a research project would involve studying organizations operating in different industries across the economy.

Another limitation of this research may be attributed to the use of theory of contextualist strategic change in addressing the research problem. The use of this particular theory has indeed provided a rich understanding of the phenomenon of information systems security change in organizations. Alternatively, we may employ other equally promising theories to understand the problem. One such possible future research direction might be the use of institutional theory in studying security failures in organizations.

8.2.2. Methodological issues

This research was conducted in an interpretive tradition. The tenets of interpretivism were firmly adhered with. The evaluation of this dissertation based upon the set of interpretive principles advanced by Klein and Myers (1999) is detailed in Table 8.1. However, advocates of other research approaches such as positivism might not necessarily agree with the underlying principles of interpretivism. As such, the use of interpretive approach in this research may be considered to be a limitation by certain

research community. However, we must opt for eclecticism with systematic inquiry rather than restrict ourselves to a singular view of world. The aim should be to resolve the research problem. The interpretive approach has been used in this research because it is sympathetic to the exploratory nature of the research study. Further research studies may be conducted that follow positivist or realist approach to confirm the findings of this dissertation. These confirmatory research studies may alternatively employ research methods other than the case study.

Table 8.1: Evaluation of dissertation

Klein and Myers (1999) criteria	Dissertation Research
The Hermeneutic Circle	It is difficult to provide explicit evidence for this criterion as it is implicit to the process. The evidence provided for rest of the criteria may be used to satisfy this criterion. The focus of this study has been on the details of an act that form an event and the intuited wholeness of that event.
Contextualization	This criterion is the very core of this research. The study has operated within the paradigm of contextualism. The theory used to investigate the research problem has also been developed from contextualism. Documents were collected that provided information about the historical context. Former stakeholders (ex-employees) were identified and interviewed to provide historical details. For instance, former CISO of both ITA and DOT were interviewed. Interviewees were asked to recollect the facts and the context surrounding an event of interest.
Interaction Between the Researchers and the Subjects	Semi-structured interviews with open ended questions were used to elicit individual interpretations of subjects. The emerging themes and key findings were discussed with an informant in each organization.
Abstraction and Generalization	Data has been interpreted using the theoretical framework. General themes were developed based upon data interpretation and related to social action in terms of security. Frameworks, models and principles for effecting security change have been provided. An overall theory for successful organizational security transformation has been developed.
Dialogical Reasoning	Initial conceptions about the Theory of Contextualist Strategic Change were revised to use the theory as a meta-theory. Bourdieu's cultural theory, structurational theory and action theory were used to understand the inter-relationship between the main theoretical components of the original theory. Generation of themes and subsequent discussion involved careful revision with respect to the theoretical assumptions.
Multiple Interpretations	Different stakeholder groups were identified and members interviewed. Members belonging to a particular group emphasized interpretations to enhance the interests of their group. For instance, there was prominent difference in expectations of security group, non-security IT group, and non-IT group.
Suspicion	Data was collected using both primary and secondary sources to reduce potential distortion of facts. In addition, multiple members within different stakeholder groups were interviewed. This was done to check for any potential bias and distortions in accounts of a particular event of interest. Emergent themes and findings were also discussed with an informant in each organization.

REFERENCES

REFERENCES

- Adams, D.A., R.R. Nelson, and P.A. Todd (1992). "Perceived Usefulness, Ease of Use, and Usage of Information Technology: A Replication." *MIS Quarterly*, 16(2): 227-247.
- Adams, D.A., and S.Y. Chang (1993). "An investigation of keypad interface security." *Information & Management*, 24(2): 53-59.
- Alter, S. (1978). Development Patterns for Decision Support Systems. *MIS Quarterly*, 2(3): 33-42.
- Ang, C., M.A. Davies, and P.N. Finlay (2001). "An empirical model of IT usage in the Malaysian public sector." *The Journal of Strategic Information Systems*, 10(2): 159.
- Ariss, S.S. (2002). "Computer monitoring: benefits and pitfalls facing management." *Information & Management*, 39(7): 553-558.
- Argyris, C., and D.A. Schon (1974). *Theory in Practice: Increasing Professional Effectiveness*. San Francisco: Jossey-Bass.
- Argyris, C., R. Putnam, and D.M. Smith (1985). *Action Science: Concepts, Methods, and Skills for Research and Intervention*. San Francisco: Jossey-Bass.
- Avgerou, C. (2001). "The significance of context in information systems and organizational change." *Information Systems Journal*, 11(1): 43-63.
- Backhouse, J., C.W. Hsu, and L. Silva (2006). "Circuits of power in creating de jure standards: shaping an international information systems security standard." *MIS Quarterly*, 30(August): 413.
- Barki, H., S. Rivard, and J. Talbot (1988). "An Information Systems Keyword Classification Scheme." *MIS Quarterly*, 12(2): 299.
- Baroudi, J.J. (1991). "Studying information technology in organizations: Research approaches and assumptions." *Information Systems Research*, 2(1): 1.

- Barrett, M. and G. Walsham (1999). "Electronic Trading and Work Transformation in the London Insurance Market Source", *Information Systems Research*, 10(1): 1 – 22.
- Baskerville, R., and M. Siponen (2002). "An information security meta-policy for emergent organizations." *Logistics Information Management*, 15(5/6): 337.
- Benbasat, I. (2001). Editorial note. *Information Systems Research*, 12: iii-iv.
- Benbasat, I., D. Goldstein, and M. Mead (1987). "The case research strategy in studies of information systems." *MIS Quarterly*, 11(3): 369-386.
- Biros, D.P., J.F. George, and R.W. Zmud (2002). "Inducing sensitivity to deception in order to improve decision making performance: A field study." *MIS Quarterly*, 26(2): 119.
- Blaikie, N. (1993). *Approaches to social enquiry*. Cambridge, MA: Blackwell Publishers Inc.
- Boockholdt, J.L. (1987). "Security and integrity controls for microcomputers: A summary analysis." *Information & Management*, 13(1): 33-41.
- Boockholdt, J.L. (1989). "Implementing security and integrity in micro-mainframe networks." *MIS Quarterly*, 13(2): 135.
- Bourdieu, P. (1991). *Language and Symbolic Power*. J. Thompson (ed.), Translator G. Raymond and M. Adamson. Cambridge, Mass: Harvard University Press.
- Bourdieu, P. (1990). *The Logic of Practice*. Stanford: Stanford University Press.
- Bourdieu, P. (1989). "Social space and symbolic power." *Sociological Theory*, 7(1): 14-25.
- Bourdieu, P. (1986). "The forms of capital." In J.G. Richardson (ed.), *Handbook of Theory and Research for the Sociology of Education*. New York: Greenwood Press.
- Bourdieu, P. (1985). "The genesis of the concepts of "habitus" and "field."" *Sociocriticism*, 2(2): 11-24.
- Bourdieu, P. (1984). *Distinction: A Social Critique of the Judgement of Taste*. Cambridge, MA: Harvard University Press.
- Bourdieu, P. (1983). "The field of cultural production, or the economic world reversed." *Poetics*, 12: 311-356.

Bourdieu, P. (1977). *Outline of a Theory of Practice*. Cambridge: Cambridge University Press.

Bourdieu, P. (1971). "Intellectual field and creative project." In M.F.D. Young (ed.), *Knowledge and Control: New directions for the sociology of education*. London: Collier-Macmillan.

Bourdieu, P., and L.J.D. Wacquant (1992). *An Invitation to Reflexive Sociology*. Chicago: University of Chicago Press.

Bourdieu, P., and J. Passeron (1977). *Reproduction in Education, Society and Culture*. London: Sage.

Burrell, G., and G. Morgan (1979). *Sociological paradigms and organizational analysis: elements of the sociology of corporate life*. Burlington, VT: Ashgate Publishing Company.

Bussolati, U., and G. Martella (1981). "Treating data privacy in distributed systems." *Information & Management*, 4(6): 305-315.

Byrd, T.A., K.L. Cossick, and R.W. Zmud (1992). "A Synthesis of Research on Requirements Analysis and Knowledge Acquisition Techniques." *MIS Quarterly*, 16(1): 117-138.

Caldeira, M.M., and J.M. Ward (2002). "Understanding the successful adoption and use of IS/IT in SMEs: an explanation from Portuguese manufacturing industries." *Information Systems Journal*, 12(2): 121-152.

Cavusoglu, H., B. Mishra, and S. Raghunathan (2005). "The value for intrusion-detection systems in information technology security architecture." *Information Systems Research*, 16(1): 28.

Chau, P. K. Y. (1996). "An empirical assessment of a modified technology acceptance model." *Journal of Management Information Systems*, 13(2), 185-204.

Cheal, D. (2005). *Dimensions of Sociological Theory*. Basingstoke: Palgrave Macmillan.

Choudhury, V. (1997). "Strategic choices in the development of interorganizational information systems." *Information Systems Research*, 8(1): 1.

Colter, M.A. (1984). "A Comparative Examination of Systems Analysis Techniques." *MIS Quarterly*, 8(1): 51-66.

- Dahlbom, B., and L. Mathiassen (1993). *Computers in Context: The Philosophy and Practice of Systems Design*. Malden, MA: Blackwell Publishing.
- Davis, F. D. (1989). "Perceived Usefulness, Perceived Ease of Use and User Acceptance of Information Technology." *MIS Quarterly* (13:3), 1989, pp. 319-339.
- Davis, F. D., Bagozzi, R. P., and Warshaw, P. R. (1989). "User Acceptance of Computer Technology: A Comparison of Two Theoretical Models." *Management Science*, 35(8): 982-1002.
- Denzin, N.K., and Y.S. Lincoln (2000). "The discipline and practice of qualitative research." In N.K. Denzin and Y.S. Lincoln (Eds.), *Handbook of Qualitative Research*, 2nd edition. Thousand Oaks, CA: SAGE Publications, Inc.
- Dhillon, G. (1995). *Interpreting the Management of Information Systems Security*, Doctoral dissertation, London School of Economics and Political Science.
- Dhillon, G., and J. Backhouse (2001). "Current directions in IS security research: towards socio-organizational perspectives." *Information Systems Journal*, 11(2): 127-153.
- Dhillon, G., and Torkzadeh, G. (2006). "Value-focused assessment of information system security in organizations." *Information Systems Journal*, 16: 293.
- Dishaw, M. T., and D.M. Strong (1999). "Extending the technology acceptance model with task-technology fit constructs." *Information & Management*, 36(1), 9-21.
- Doherty, N.F., and H. Fulford (2006). "Aligning the information security policy with the strategic information systems plan." *Computers & Security*, 25: 55-63.
- Ein-Dor, P., and Segev, E. (1993). "A classification of information systems analysis and interpretation." *Information Systems Research*, 4(2): 166.
- Eisenhardt, K. (1989). "Building theories from case study research." *Academy of Management Review*, 14(4): 532-550.
- Frank, J., B. Shamir, and W. Briggs (1991). "Security-related behavior of PC users in organizations." *Information & Management*, 21(3): 127-135.

- Gable, G.G. (1994). "Integrating case study and survey research methods: an example in information systems." *European Journal of Information Systems*, 3(2): 112-126.
- Gal-Or, E., and A. Ghose (2005). "The Economic incentives for sharing security information." *Information Systems Research*, 16(2): 186.
- Gao, P. (2005). "Using actor-network theory to analyse strategy formulation." *Information Systems Journal*, 15(3), 255–275.
- Gefen, D., and D.W. Straub (1997). "Gender differences in the perception and use of E-mail: An extension to the technology acceptance model." *MIS Quarterly*, 21(4): 389-400.
- Giddens, A. (1993). *The Transformation of Intimacy*. Stanford, CA: Stanford University Press.
- Giddens, A. (1984). *The Constitution of Society: Outline of the Theory of Structuration*. Cambridge: Polity Press.
- Giddens, A. (1979). *Central Problems in Social Theory: Action, Structure and Contradiction in Social Analysis*. London: Macmillan.
- Giddens, A. (1976). *New Rules of Sociological Method*. London: Hutchinson.
- Golden-Biddle, K., and K. Locke (1993). "Appealing work: An investigation of how ethnographic texts convince." *Organization Science*, 4(4): 595-616.
- Goldstein, R.C., and V.C. Storey (1992). "Unravelling is-a structures." *Information Systems Research*, 3(2): 99.
- Goodhue, D.L., and D.W. Straub (1991). "Security concerns of system users: A study of perceptions of the adequacy of security." *Information & Management*, 20(1): 13-27.
- Grenfell, M., and D. James (1998). *Bourdieu and Education: Acts of Practical Theory*. New York, NY: Routledge.
- Guba, E.G. (1990). "The alternative paradigm dialog." In E.G. Guba (Editor), *The paradigm dialog*. Newbury Park, CA: SAGE Publications, Inc.
- Guba, E.G., and Y.S. Lincoln (1989). *Fourth Generation Evaluation*. Newbury Park, CA: SAGE Publications, Inc.

- Gupta, A., Y.A. Tung and J.R. Marsden (2004). "Digital signature: use and modification to achieve success in next generational e-business processes." *Information & Management*, 41(5): 561-575.
- Harrington, S.J. (1996). "The effect of codes of ethics and personal denial of responsibility on computer abuse judgments and intentions." *MIS Quarterly*, 20(3): 257.
- Hayes, S.C., L.J. Hayes, and H.W. Reese (1988). "Finding the philosophical core: A review of Stephen C. Pepper's world hypotheses: A study in evidence." *Journal of the Experimental Analysis of Behavior*, 50(1): 97.
- Held, D., and J.B. Thompson (eds) (1989). *Habermas: Critical Debates*. Cambridge: Cambridge University Press.
- Igbaria, M., T. Guimaraes, and G.B. Davis, (1995). "Testing the determinants of microcomputer usage via a structural equation model." *Journal of Management Information Systems*, 11(4): 87-114.
- Igbaria, M., N. Zinatelli, P. Cragg, and A.L.M. Cavaye (1997). Personal computing acceptance factors in small firms: A structural equation model. *MIS Quarterly*, 21(3), 279-305.
- Iivari J. (1991), A paradigmatic analysis of contemporary schools of IS development, *European Journal of Information Systems*, 1(4): 249-272.
- Iivari, J., R. Hirschheim, and H.K. Klein (1998). "A paradigmatic analysis contrasting information systems development approaches and methodologies." *Information Systems Research*, 9(2): 164.
- Irani, Z., P.E.D. Love, T. Elliman, S. Jones, and M. Themistocleous (2005). "Evaluating e-government: learning from the experiences of two UK local authorities." *Information Systems Journal*, 15(1), 61-82.
- Jackson, C. M., S. Chow, and R.A. Leitch (1997). "Toward an understanding of the behavioral intention to use an information system." *Decision Sciences*, 28(2), 357-389.
- Jung, B., I. Han, and S. Lee (2001). "Security threats to Internet: a Korean multi-industry investigation." *Information & Management*, 38(8): 487-498.
- Karyda, M., E. Kiountouzis, and S. Kokolakis (2005). "Information systems security policies: a contextual perspective." *Computers & Security*, 24: 246-260.

- Katos, V. and C. Adams (2005). "Modelling corporate wireless security and privacy." *The Journal of Strategic Information Systems*, 14(3): 307-321.
- Klein, H.K., and M.D. Myers (1999). "A set of principles for conducting and evaluating interpretive field studies in information systems." *MIS Quarterly*, 23(1): 67-94.
- Kling, R. (1980). "Computer abuse and computer crime as organizational activities." *Computer Law Journal*, 2(2): 186-196.
- Kotulic, A.G., and J.G. Clark (2004). "Why there aren't more information security research studies." *Information & Management*, 41(5): 597-607.
- Lawley, E.L. (1994). "The sociology of culture in computer mediated communication: An initial exploration." Accessed at <http://www.its.com/elawley/bourdieu.html>, on September 14, 2007.
- Lee, A.S. (2004). "Thinking about social theory and philosophy for information systems." In J. Mingers and L. Willcocks (Eds), *Social Theory and Philosophy for Information Systems*, pp. 1-26. Hoboken, NJ: John Wiley & Sons.
- Lee, A.S. (1999). "Researching MIS." In W.L. Currie and B. Galliers (Eds), *Rethinking Management Information Systems*, pp. 7-27. New York: Oxford University Press.
- Lee, A.S. (1991). "Integrating positivist and interpretive approaches to organizational research." *Organization Science*, 2(4): 342-365.
- Lee, A.S. (1989). "A scientific methodology for MIS case studies." *MIS Quarterly*, 13(1): 33-52.
- Liang, H., and Y. Xue (2004). "Coping with ERP-related contextual issues in SMEs: a vendor's perspective." *The Journal of Strategic Information Systems*, 13(4): 399.
- Liebenau, J., and J. Backhouse (1990). *Understanding Information*. London: Macmillan.
- Loch, K.D., H.H. Carr, and M. E. Warkentin (1992). "Threats to information systems: Today's reality, yesterday's understanding." *MIS Quarterly*, 16(2): 173.
- Lucas, H. C., Jr, and V.K. Spitler (1999). "Technology use and performance: A field study of broker workstations." *Decision Sciences*, 30(2): 291-311.
- Madison, G. B. (1988). *The Hermeneutics of Postmodernity: Figures and Themes*. Bloomington: Indiana University Press.

- Mahar, C., R. Harker, and C. Wilkes (1990). In R. Harker, C. Mahar & C. Wilkes (eds), *An Introduction to the Work of Pierre Bourdieu: the practice of theory*. London: Macmillan Press.
- Mao, J., and I. Benbasat (1998). "Contextualized access to knowledge: theoretical perspectives and a process-tracing study." *Information Systems Journal*, 8(3): 217–239.
- Marshall, C. (1990). "Goodness criteria: Are they objective or judgment calls?" In E.G. Guba (Ed.), *The Paradigm Dialog*, pp. 188-197. Newbury Park, CA: SAGE Publications, Inc.
- Mathieson, K. (1991). "Predicting user intentions: Comparing the technology acceptance model with the theory of planned behavior." *Information Systems Research*, 2(3): 173-191.
- Meyer, M. H., and K.F. Curley (1991). "An Applied Framework for Classifying the Complexity of Knowledge-Based Systems." *MIS Quarterly*, 15(4): 454.
- Mintzberg, H. (1987). "Crafting strategy." *Harvard Business Review*, July-August: 66-75.
- Morin, J., and M. Pawlak (2006). "Towards a Global Framework for Corporate and Enterprise Digital Policy Management." *Journal of Information System Security*, 2(2): 15.
- Murray, T.J. (1979). "Cryptographic transformation of data relationships." *Information & Management*, 2(3): 95-98.
- Myers, M.D. (1997). "Qualitative Research in Information Systems." *MIS Quarterly* 21(2): 241-242. *MISQ Discovery*, updated version, last modified: November 15, 2006, http://www.misq.org/discovery/MISQD_is_world/.
- Nandhakumar, J., M. Rossi, and J. Talvinen (2005). "The dynamics of contextual forces of ERP implementation." *Journal of Strategic Information Systems*, 14 (2): 221–242.
- Necco, C. R., C.L. Gordon, and N.W. Tsai (1987). "Systems analysis and design: current practices." *MIS Quarterly*, 11(4): 461.
- Nolan, R.L., and J.C. Wetherbe (1980). "Toward a Comprehensive Framework for MIS Research." *MIS Quarterly*, 4(2): 1-19.

- Orlikowski W, and J.J. Baroudi (1991). "Studying Information Technology in Organizations: Research Approaches and Assumptions." *Information Systems Research*, 2: 1-28.
- O'Brien, S., and O' Fathaigh (2005). "Bringing in Bourdieu's theory of social capital: Renewing learning partnership approaches to social inclusion." Presented at the *ESAI Annual Conference*, NUI Maynooth, April 1-3.
- Payne, R.L. (1975). "Epistemology and the study of behavior in organizations." Unpublished memo No. 68 MRC, Social & Applied Psychology Unit, University of Sheffield.
- Payne, C. (2002). "On the security of open source software." *Information Systems Journal*, 12: 61-78.
- Pepper, S.C. (1970). *World Hypotheses: A study in evidence*. Los Angeles, California: University of California Press.
- Pettigrew, A.M. (1990). "Longitudinal field research on change: Theory and practice." *Organization Science*, 1(3): 267-292.
- Pettigrew, A.M. (1985). "Contextualist research and the study of organizational change processes." In E. Mumford, R. Hirschheim, G. Fitzgerald, and T. Wood-Harper (Editors), *Research methods in information systems*. North-Holland: Elsevier Science Publishers.
- Pettigrew, A.M. (1987). "context and action in the transformation of the firm." *Journal of Management Studies*, 24(6): 649-670.
- Post, G., and A. Kagan (2000). "Management tradeoffs in anti-virus strategies." *Information & Management*, 37(1): 13-24.
- Posthumus, S., and R. von Solms (2004). "A framework for the governance of information security." *Computers & Security*, 23(8): 638-646.
- Quinn, J.B. (1995). In Mintzberg, H., and J.B. Quinn (Eds). *The Strategy Process: Concepts, Context and Cases*, 3rd Edition. Prentice Hall.
- Roos, H. (1981). "Confidentiality of information." *Information & Management*, 4(1): 17-21.
- Ryan, S.D., and B. Bordoloi (1997). "Evaluating security threats in mainframe and client/server environments." *Information & Management*, 32(3): 137-146.

- Sarason, Y. (1995). "A model of organizational transformation: The incorporation of organizational identity into a structuration theory framework." *Academy of Management Journal, Best Paper Proceedings 1995*: 47-51.
- Sarathy, R., and K. Muralidhar (2002). "The security of confidential numerical data in databases." *Information Systems Research*, 13(4): 389.
- Scalet, S. (2005). "Five steps to an effective strategic plan." *CSO*, 1 July 2005. Magazine online. Available from <http://www.csoonline.com/read/070105/fivesteps.html>. Accessed 14 Jun 2007.
- Schutz, A. (1954). "Concept and theory formation in the social sciences." *The Journal of Philosophy*, LI(9): 257 – 273.
- Schwandt, T.R. (1990). "Paths to inquiry in the social disciplines: Scientific, constructivist, and critical theory methodologies." In E.G. Guba (Ed.), *The Paradigm Dialog*, pp. 258-276. Newbury Park, CA: SAGE Publications, Inc.
- Senn, J.A. (1978). "A Management View of Systems Analysts: Failures and Shortcomings." *MIS Quarterly*, (2: 3), pp. 25-32.
- Shanks, G. (1997). "The challenges of strategic data planning in practice: an interpretive case study." *The Journal of Strategic Information Systems*, (6:1), pp. 69.
- Smith, J.K., and D.K. Deemer (2000). "The problem of criteria in the age of relativism." In N.K. Denzin and Y.S. Lincoln (Eds.), *Handbook of Qualitative Research*, 2nd edition, pp. 877-898. Thousand Oaks, CA; SAGE Publications, inc.
- Smith, H. J., S.J. Milberg, and S.J. Burke (1996). "Information privacy: Measuring individuals' concerns about organizational practices." *MIS Quarterly*, 20(2): 167.
- Stabell, C.B. (1987). "Decision support systems: alternative perspectives and schools Source." *Decision Support Systems*, 3(3): 243-251.
- Stake, R.E. (2000). *The Art of Case Study Research*, Thousand Oaks, CA: SAGE Publications, Inc.
- Straub, D.W., and R.J. Welke (1998). "Coping with systems risk: Security planning models for management decision making." *MIS Quarterly*, 22(4): 441.
- Straub, D.W., and W.D. Nance, Jr. (1990). "Discovering and disciplining computer abuse in organization." *MIS Quarterly*, 14(1): 45.

- Sun, L., R.P. Srivastava, and T.J. Mock (2006). "An information systems security risk assessment model under the Dempster-Shafer theory of belief functions." *Journal of Management Information Systems*, 22(4):109.
- Swanson, E.B., and M.J. Culnan (1978). "Document-based systems for management planning and control: A classification survey, and assessment." *MIS Quarterly*, 2(4): 31.
- Swartz, D. (1997). *Culture & power: The sociology of Pierre Bourdieu*. Chicago: The University of Chicago Press.
- Swingewood, A. (1991). *A Short History of Sociological Thought*, 2nd Edition. London: Macmillan.
- Szajna, B. (1994). "Software evaluation and choice: Predictive validation of the technology acceptance instrument." *MIS Quarterly*, 18(3), 319-324.
- Tan, J.K.H. & I. Benbasat (1990). "Processing of graphical information: A decomposition taxonomy to match data extraction tasks and graphical representations." *Information Systems Research*, 1(4): 394.
- Taylor, S., and P. Todd (1995). "Assessing IT usage: The role of prior experience." *MIS Quarterly*, 19(4): 561-570.
- Thuraisingham, B. (1993). "Multilevel security for information retrieval systems." *Information & Management*, 24(2): 93-103.
- Thuraisingham, B. (1995). "Multilevel security for information retrieval systems – II." *Information & Management*, 28(1): 49-61.
- Trauth, E.M., and L.M. Jessup (2000). "Understanding computer mediated discussions: Positivist and interpretive analysis of group support system use." *MIS Quarterly*, 24(1): 43-79.
- Turn, R. (1987). "Privacy protection in record-keeping systems." *Information & Management*, 1(4): 187-197.
- Van Maanen, J. (1979). "The fact of fiction in organizational ethnography." *Administrative Science Quarterly*, 24 (4): 539 – 550.
- Venkatesh, V., and F.D. Davis (1996). "A model of the antecedents of perceived ease of use: Development and test." *Decision Sciences*, 27(3): 451-481.

- von Solms, B. (2005). "Information security governance: COBIT or ISO 17799 or both?" *Computers & Security*, 24:99-104.
- von Solms, R., and S.H. von Solms (2006). "Information security governance: Due care." *Computers & Security*, 25(7): 494-497.
- von Solms, R., H. van der Haar, S.H. von Solms, and W.J. Caelli (1994). "A framework for information security evaluation." *Information & Management*, 26(3):143-153.
- Wagner, E.L., and S. Newell (2004). " 'Best' for whom?: the tension between 'best practice' ERP packages and diverse epistemic cultures in a university context." *The Journal of Strategic Information Systems*, 13(4): 305.
- Walsham, G. (1993). *Interpreting Information Systems*. Chichester: John Wiley & Sons.
- Walsham, G. (1995). "Interpretive case studies in IS research: nature and method." *European Journal of Information Systems*, 4(2): 74-81.
- Walsham, G., and S. Sahay (1999). "GIS for district level administration in India: Problems and opportunities." *MIS Quarterly*, 23(1): 39-66.
- Ward, J., and R. Elvin (1999). "A new framework for managing IT-enabled business change." *Information Systems Journal*, 9(3): 197-221.
- Weiss, I.R. (1980). "Auditability of software: A survey of techniques and costs." *MIS Quarterly*, 4(4): 39.
- Wetherbe, J.C., and C.J. Whitehead (1977). "A Contingency View of Managing the Data Processing Organization." *MIS Quarterly*, 1(1): 19-25.
- Wijnhoven, F., T. Spil, R. Stegwee, and R.T.A. Fa (2006). "Post-merger IT integration strategies: An IT alignment perspective." *The Journal of Strategic Information Systems*, 15(1): 5.
- Wilson, M., and D. Howcroft (2005). "Power, politics and persuasion in IS evaluation: a focus on 'relevant social groups'." *The Journal of Strategic Information Systems*, 14(1): 17.
- Yin, R.K. (1989). *Case study research: Design and methods*, Newbury Park, CA: SAGE Publications, Inc.

Yiu, S.M., S.W. Yiu, L.K. Lee, E.K.Y. Li, and M.C.L. Yip (2006). "Sharing and access right delegation for confidential documents: A practical solution." *Information & Management*, 43: 607-616.

Zviran, M., and W.J. Haga (1999). "Password security: An empirical study." *Journal of Management Information Systems*, 15(4): 161.

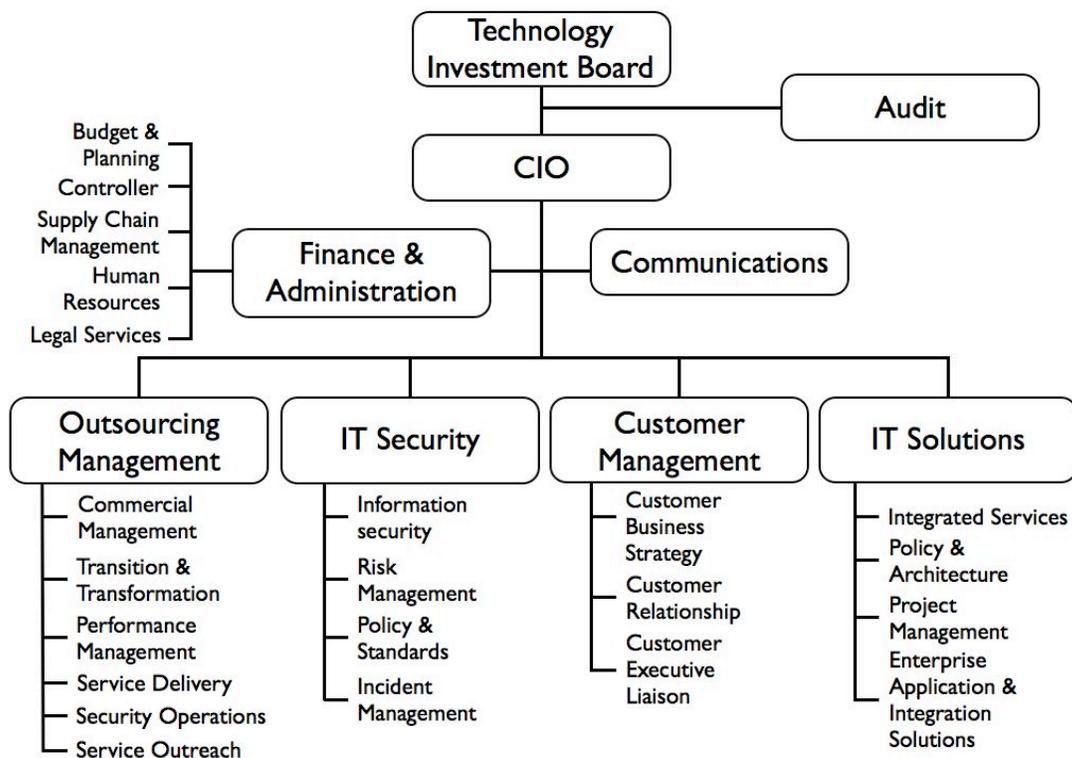
APPENDIX A
Information Technology Agency
Case Study: Interviews conducted

Time period spent at the field site: November 2006 to September 2007

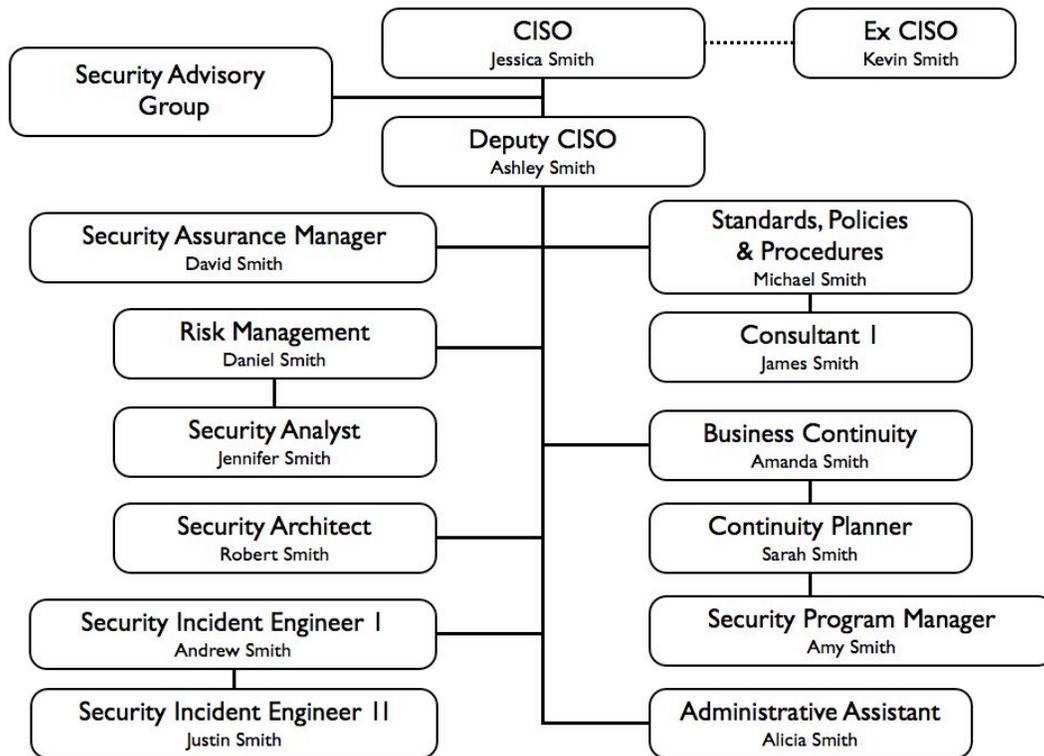
Number of organizational members formally interviewed: 33

Additional sources of observation for organizational operations: Staff meetings, committee meetings, advisory council meetings, informal meetings.

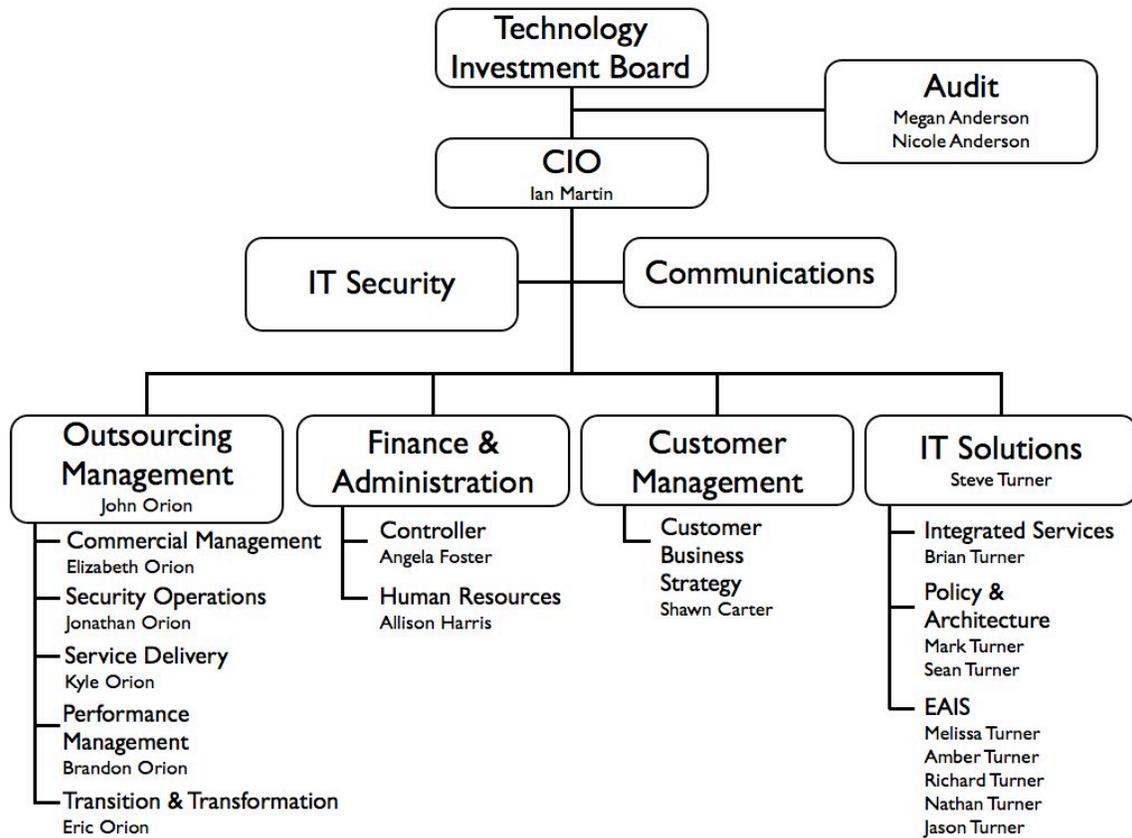
Organizational structure:



Formal in-depth meetings conducted with the organizational members from the IT Security directorate:



Formal in-depth meetings conducted with the organizational members from other directorates:



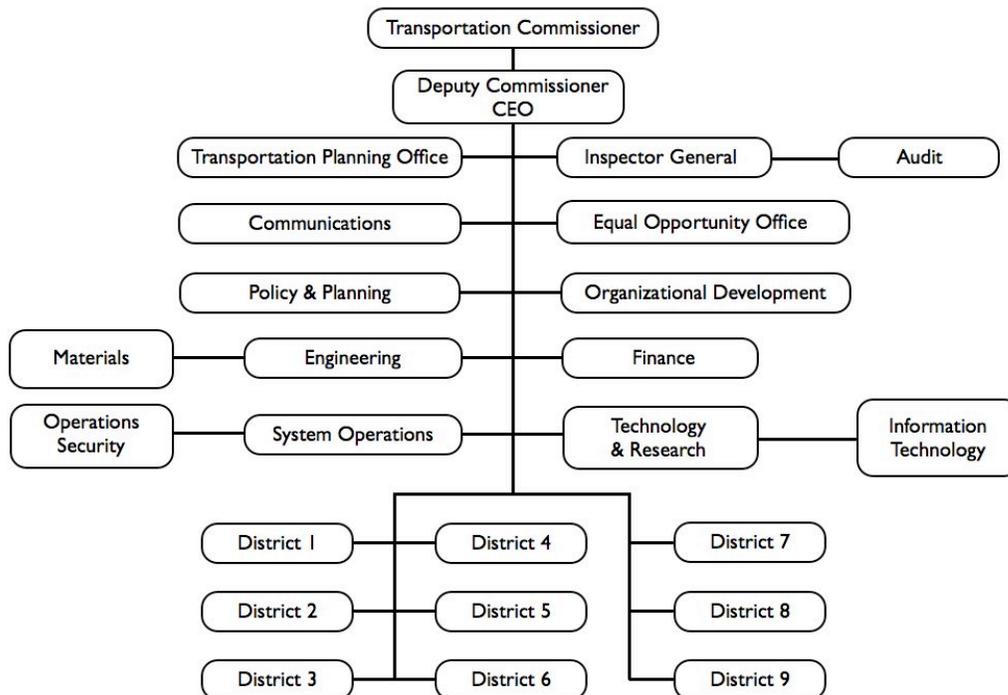
Appendix B
Department of Transportation
Case Study: Interviews conducted

Time period spent at the field site: April 2007 to September 2007

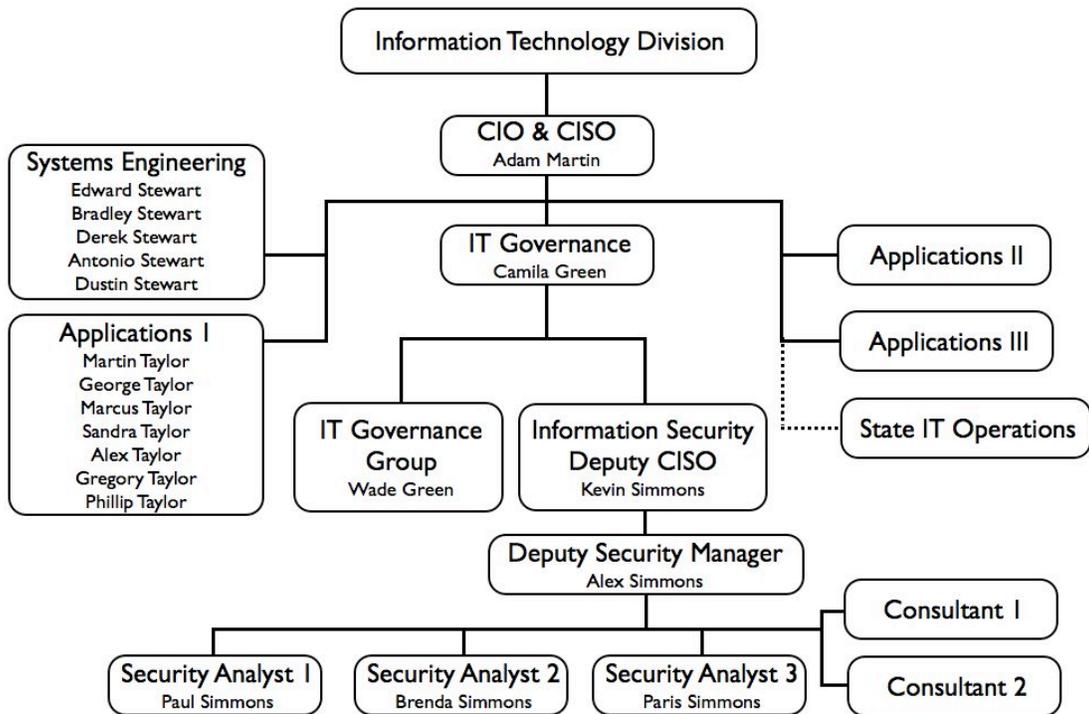
Number of organizational members formally interviewed: 28

Additional sources of observation for organizational operations: Group meetings, informal meetings.

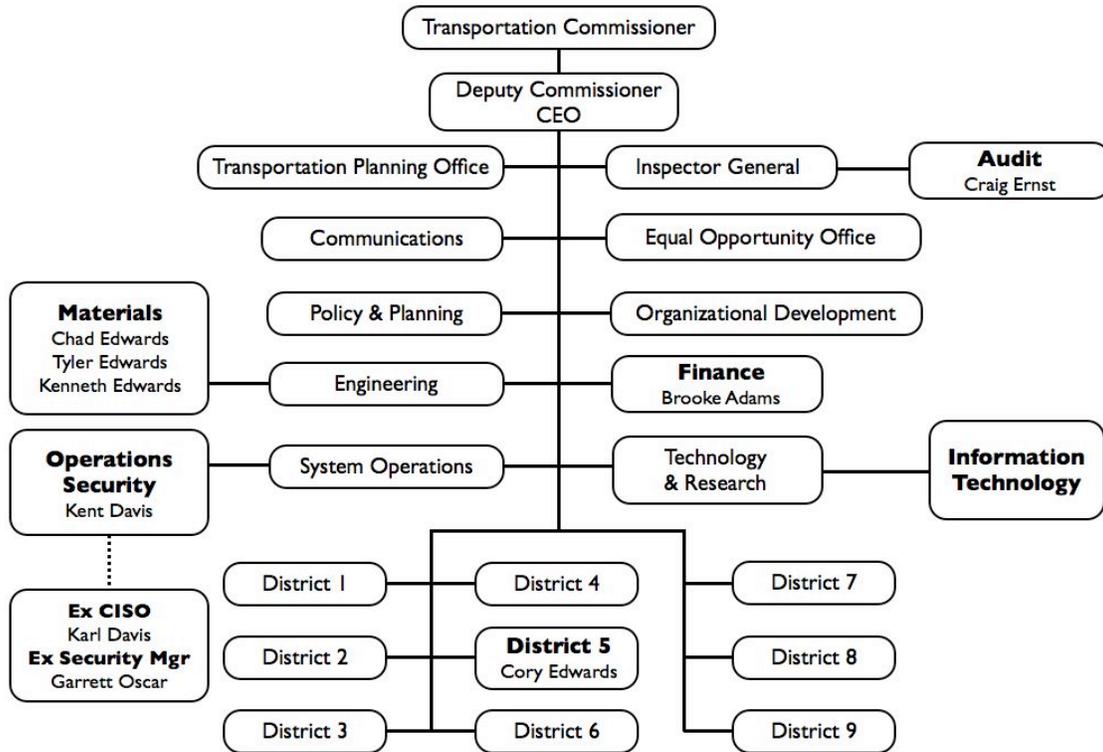
Organizational structure:



Formal in-depth meetings conducted with the organizational members from the Information Technology Division:



Formal in-depth meetings conducted with the organizational members from other divisions:



APPENDIX C

Topic Guide

Questions inquiring about the context

1. What is your perception about information system security at the organization?
2. What do you consider to be the issues or concerns with security efforts at the organization?
3. What is the security governance structure?
4. What governance structure would you like to see to deal with your organization's complexity?
5. Why is the security council being developed?
6. What are the challenges in dealing with political dynamics both internally and externally?
7. How has your organization adapted to previous technology related changes?
8. What is your perception about security culture at your organization?
9. What are the roles and responsibilities of various security members?
10. What are the resources with agencies to implement the security program?
11. Do the agencies have control over the resources required for successful implementation of the security program?
12. Identify alternative strategy (or action plan) for an organization where there is a so-to-speak merger of 92 organizations (in terms of IT infrastructure) and also, outsourcing arrangement.
13. What do you consider to be the success measures for the security efforts.
14. Do you think security group is meeting the expectations of organizational members?

15. Were you convinced by the argument provided by the security group for making security prominent?
16. What are the important factors to give a program or policy a strategic thrust?
17. What is the financial model followed by this organization when it comes to services provided? Does the organization have budget allocation from the state?
18. What would you consider to be the key traits for a CSO in order to navigate the complex environment?
19. What is the logic for current security approach? Basically, why this approach?
20. Is the security program being adopted based upon their success in other existing organizations?
21. Who do you think are the powerful people when it comes to information security?
22. What are the factors that did favor or impede introduction of security program?
23. What are the possible points of strain within organization?
24. What are the future aims of the security efforts?

Questions inquiring about the content

1. Have you read information security policy?
2. What is your opinion about the security policy adopted by the security group?
3. What is your understanding about information security program?
4. What is your understanding about the security initiatives introduced?
5. What are the various components of the security program?
6. Have you undergone security training?
7. Are you aware about information security at your organization?
8. Have you seen any security (awareness) initiatives at your organization?
9. What is your opinion on the significance of information security?
10. What do you consider to be the role of security?
11. From your point of view, what is the most significant security issue?
12. How can we improve security program?

13. What would you like to change in security efforts at your organization? Are you happy with the strategy adopted by security group?
14. What is the role and focus of the security department?
15. What are the goals and objectives for your organization's security?
16. Why the particular areas of need have been identified?
17. What constitutes the compliance program?
18. How is the security awareness training provided to organizational members?

Questions inquiring about the process

1. In your opinion, has security role been used in exercise of control?
2. Did security impact institutional order?
3. How do you ensure information security while doing your regular work?
4. Are we on right track in terms of information security approach at your organization?
5. If I were to ask you to institute information security at your organization what would be your response? How would you do it?
6. What would be your approach to institute security at your organization?
7. What are the important factors to achieve success?
8. What would make you abide by the security program and make it successful?
9. What would you like to change in the security approach adopted at your organization?
10. What would be your top two issues or concerns associated with security endeavor at your organization?
11. Have you faced any changes in your work with introduction of information security controls?
12. Have you noticed any changes in the way things used to be done with introduction of security at your organization?
13. What do you believe to be the drivers of information security at your organization?

14. How did employees react to security initiatives? Any resistance?
15. How has information security been received at your organization? Has it been adopted wholly?
16. Did security create adverse situation at your organization?
17. What are the issues that need to be dealt with while instituting a program in an organization like your organization?
18. How has information security been received at your organization?
19. How is the security program being formulated?
20. How is the security program being implemented?
21. What are the actions that have been taken to develop the program?
22. How has your organization adapted to previous IS security attempts?
23. How is the security group acting on the employee reactions?
24. Have any initiatives been undertaken to interact with organizational members?
25. What are the negotiations or maneuvers that accompanied formulation and implementation of security program?
26. What new alliances were required for implementing security program?
27. What is the management process for decision-making?
28. What are the mechanisms of control exerted over the organizational members when they perform their activities?

Vita

Gurvirender Pal Singh Tejay was born on December 20th, 1975 at Deolali in the western state of Maharashtra in India. He holds an Indian citizenship. He came to the United States in 1999 to pursue undergraduate education. He received his Bachelor of Arts in Economics from the University of Wisconsin, Milwaukee in December 2000. He was awarded a Non-Resident Tuition Remission award by the University for the duration of his undergraduate studies. During his studies, he was selected for the Deans Honor List and graduated with Magna Cum Laude and Gold Chord-Commencement Honors. Gurvirender went on to receive a Masters of Arts in Economics from the same university in 2002. He was awarded a graduate teaching assistantship for his studies in the program. Upon graduation, he decided to pursue his interest in information technology. He received a Masters of Science in Computer Science from the University of Chicago in 2003.

Gurvirender was accepted for the doctoral program in information systems at the Virginia Commonwealth University (VCU) in the fall of 2003. As a doctoral student, he was awarded a graduate teaching assistantship for the degree program. Gurvirender served as an Adjunct Instructor at VCU from September 2005 to August 2006. During his tenure at VCU, he has taught Introduction to Object Oriented Programming, Introduction to Information Systems, Projects in Java, Database Systems and Information Systems Planning. In 2006, Gurvirender also served as an Information Security Policy Consultant for the Virginia Information Technology Agencies through Information Systems Research Institute at VCU.

Gurvirender is currently serving as an Assistant Professor at the Nova Southeastern University (NSU) in Ft. Lauderdale, Florida where he has been employed since 2007. At NSU, he has taught Information Security Management, Information Security Policy, Privacy and Ethics, Information Security Project, and Information Systems Project Management.

Gurvirender has been conducting research in information systems security, information quality and information systems strategy. He has presented his research work at several leading information systems conferences including Americas Conference on Information Systems, Hawaii International Conference on System Sciences and International Federation for Information Processing conference. His publications include:

Tejay, G., Coss, D., and Dhillon, G. (2007). "Interpreting IT implementation initiatives in an organization: A cultural perspective." International Federation for Information Processing (IFIP) Working Group 8.2 research workshop - Organizations and Society in Information Systems (OASIS) 2007, Montreal, Canada.

Tejay, G. (2007). "Understanding philosophical dimensions of socio-organizational information systems security." 6th Annual Security Conference, Las Vegas, Nevada.

Dhillon, G., Tejay, G., and Hong, W. (2007). "Identifying governance dimensions to evaluate information systems security in organizations." *Hawaii International Conference on System Sciences (HICSS)*, Waikoloa, Hawaii, January.

Gupta, M., Sharman, R., and Tejay, G. (2006). "SAML based Role Hierarchy Preservation Model for Cross-enterprise Identity Federation." *The Second Secure Knowledge Management Workshop (SKM) 2006*, New York, USA.

Tejay, G. (2006). "Identifying information systems security requirements for different organizational forms: A transactions cost approach." *Twelfth Americas Conference on Information Systems (AMCIS)*, Acapulco, Mexico, August.

Lapke, M., Tejay, G., and Weistroffer, R. (2006). "Integrating security in information systems development approach: A socio-technical view." *The 5th Annual Security Conference*, Las Vegas, NV, April.

Tejay, G., Dhillon, G., and Chin, A.G. (2005). "Data Quality Dimensions for Information Systems Security: A Theoretical Exposition." In *Security Management, Integrity, and Internal Control in Information Systems*, Eds. P. Dowland, S. Furnell, B. Thuraisingham and X. S. Wang, pp 21-39. New York: Springer.

Tejay, G., and Dhillon, G. (2005). "Developing Measures of Information Security Culture." *The Fourth Annual Workshop on E-Business*, Las Vegas, NV, December.

Tejay, G. (2005). "Making Sense of Information Security Standards." In *Proceedings of Eleventh Americas Conference on Information Systems (AMCIS)*, Omaha, NE, August.

Tejay, G. (2004). "Information Security Standards." *The 4th Annual Security Conference*, Las Vegas, NV, April.