2012

ALIGNING SECURITY AND USABILITY OBJECTIVES FOR COMPUTER BASED INFORMATION SYSTEMS

Santa Ram Susarapu
Virginia Commonwealth University

ALIGNING SECURITY AND USABILITY OBJECTIVES FOR COMPUTER BASED INFORMATION SYSTEMS

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

By

SANTA RAM SUSARAPU
M.B.A., University of Nebraska, 2003
B.Com., Andhra University, India, 1995

Dissertation Chair: DR. GURPREET DHILLON
PROFESSOR, DEPARTMENT OF INFORMATION SYSTEMS

Dissertation Co-Chair: DR. H. ROLAND WEISTROFFER
PROFESSOR, DEPARTMENT OF INFORMATION SYSTEMS

Virginia Commonwealth University
Richmond, Virginia

08/2012

Acknowledgements

I could not have completed this monumental task without the unconditional support of my dissertation committee chair and mentor Dr. Gurpreet Dhillon. During several ups and downs since I joined the Ph.D. program, Dr. Dhillon has been a constant inspiration and supporter and have always believed in me. I am very grateful for his continued support. I wish the Almighty showers the blessings on him and his family always.

I am very thankful for the strong support extended by my dissertation committee co-chair Dr. H Roland Weistroffer and the rest of the committee members.

My doctoral experience at VCU has also been shaped by several doctoral students, faculty and staff at VCU and I am very thankful for them for helping me with the experience.

I would also like to thank all my friends who are spread across the east and west coasts of USA and India. Especially, I would like thank the families of Dr. Ambrose Jones III, Dr. K. Niki Kunene, Dr. Elizabeth Baker, David Rafner, LaShondra Erwin Jones, Anema Harter and M. David Allen for their moral support and friendship over the last several years.

Last but not least, I am thankful for my beloved parents who have given me all the freedom to pursue what I want in life.

Finally, I thank God for all the opportunities and curveballs He has thrown at me.

Table of Contents

Chapter 7 – Conclusion 108

Abstract

ALIGNING SECURITY AND USABILITY OBJECTIVES FOR COMPUTER BASED INFORMATION SYSTEMS

By: Santa Ram Susarapu, Ph.D.

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

Dissertation Chair: DR. GURPREET DHILLON
PROFESSOR, DEPARTMENT OF INFORMATION SYSTEMS

Dissertation Co-Chair: DR. H. ROLAND WEISTROFFER
PROFESSOR, DEPARTMENT OF INFORMATION SYSTEMS

With extensive use of information systems in day-to-day business operations, many organizations are facing challenges to develop robust computer-based information systems that are secure and widely used by the user community. In order to develop information systems that are secure and useful, understanding what stakeholders consider important and value about the security and usability is critical. Security refers to confidentiality, integrity and availability and usability refers to efficiency, effectiveness and user satisfaction. Using Value Focused Thinking approach, this research first proposes the usability objectives based on the values of system developers and users. Using the security objectives proposed by Dhillon & Torkzadeh (2006) and the usability objectives, this research proposes hierarchies with the overall/over-arching goals of security (confidentiality, integrity, availability) and/or usability (efficiency, effectiveness

and satisfaction). This research also analyzes a case of computer hacking and identifies which of the security and usability objectives that have not been met in that case study. The research contributions which include the usability objectives and security and usability hierarchies can be useful for theoretical as well as practical purposes.

Chapter 1 - Introduction

1.1 Background

With extensive use of information systems in day-to-day business operations, many organizations have been experiencing significant with information systems. One such organizational challenge is developing robust computer-based information systems that are secure and widely adopted by the user community, i.e. the alignment of security and usability objectives.

In recent years, due to legal and regulatory requirements encoded in legislations such as the Health Insurance Portability and Accountability Act (HIPAA) of 1996, the Financial Services Modernization Act of 1999 (also known as Gramm–Leach–Bliley Act), the Sarbanes–Oxley Act of 2002, the Dodd–Frank Wall Street Reform and the Consumer Protection Act of 2010 and other relevant privacy regulations in the United States, information systems security and privacy of data stored in such databases become a high priority for many organizations. In 2009, The Enterprise Strategy Group, through a survey of Information Technology (IT) professionals in large companies, noted that compliance with government and industry regulations is the major factor that motivated IT professionals' decisions to improve data security (Oltsik 2009). More recently, in a 2011 Global State of Information Security Survey conducted by PricewaterhouseCoopers LLP (PwC), 55% of North American survey respondents (which included CEOs, CFOs, CIOs, CSOs, Vice-presidents and directors of IT and information security) indicated that legal and regulatory requirements are one of the leading justifications for additional investments in information security (PriceWaterhouseCoopers 2011).

There are three specific stakeholders in an organization that interact with information systems in some capacity or another: owners, developers and users. System owners and developers tend to focus on the security of the computer-based information systems and the data stored in these systems. However, users prefer ease of use with minimal security controls. These divergent views, perceptions and preferences of the system owners, developers and users have given rise to several gaps between security objectives and usability objectives incorporated into such systems.

The increasing gap between systems security and systems usability objectives is also posing several new and unforeseen risks to organizational IT environments ultimately leading to both monetary and non-monetary loses to these organizations. The information systems research and practice communities have addressed the gap in a limited manner by focusing either solely on the systems security objectives or solely on the systems usability objectives. In addition, the systems security and usability objectives heavily depend upon various concepts such as the context and purpose for which the information system is conceived, designed, developed and implemented and the nature and type of data that is stored and processed in the information system. Therefore, there is a tremendous need to understand the system objectives from the system owners, developers and users perspective and to determine the optimal balance between the security and usability objectives, as within a given organizational contexts.

Dhillon and Torkzadeh (2006) proposed information system security objectives from the system security professionals point of view. The security professionals that were studied by Dhillon & Torkzadeh (2006) included, but were not limited to system owners and developers. The current research defines the information systems usability objectives

from developer and user perspective. The purpose of this research is to explore the alignment of the security and usability objectives such that the resultant system objectives would inform the business organizations with better systems development practices and enable organizations to balance the conflicting information systems security and usability objectives within their own organizational context.

The next two sections of this chapter define the research problem at hand as well as the scope of this research. The final section of this chapter presents the structure of the dissertation.

1.2 Problem Definition

Systems security and usability along with systems development have been dominant topics of information systems research in recent years. The emerging field of Human Computer Interaction and Security (HCI-SEC) is beginning to make an impact on the systems security and systems usability communities (DeWitt and Kuljis 2006). However, most of the existing research has focused on the technical aspects of either systems security or systems usability. Moreover, in majority of the systems development methodologies, systems security and systems usability have traditionally been considered as add-ons to the end product of systems development process. Systems security and usability have not been integrated into the development process from the systems requirements analysis stage. Yee (2004) argues that "Security and usability elements cannot be sprinkled on a product like pixie dust." Highlighting the current research gaps, Yee (2004) also emphasizes that there is a compelling need for the alignment of systems security and systems usability by incorporating both security and usability throughout the system development and design processes.

If the systems security and systems usability objectives have not been aligned from the beginning and are not integrated into the development process, the users are left to make certain choices between security and usability features, which may result in trade-offs between systems security and systems usability. Such trade-off decisions by the users might not, in many cases, align with the organizational security policies, procedures and processes. It is also well known that if the information systems are made highly secure, such systems are less usable and if the information systems are made less secure, such systems are more usable (Cranor and Garfinkel 2005). In some organizational contexts, it might be completely appropriate to give system users the ability to choose between systems security and systems usability features. However, for certain organizational contexts, such as retail companies dealing with consumer credit card information, financial services organizations and defense or military establishments, there will be a point at which neither information systems security nor systems usability can be compromised beyond an optimal level. Such an optimal point of compromise for systems security and systems usability depends on a careful understanding of the systems security as well as systems usability objectives based on the perceptions of relevant stakeholders such as system owners, developers and users.

Dhillon and Torkzadeh (2006) proposed information system security objectives from the system security professional point of view. However, in the information system research, we are not aware if system usability objectives from the system users' perspectives have practically not been studied.

The basic premise for the proposed research is that many computer-based information systems are not being used or are not useful for the organizations after spending large

sums of money on their development. This research proposes that appropriate alignment of the systems security and systems usability objectives from the beginning of the system development process is a critical component for the efficient and effective use of the computer-based information systems.

In this dissertation, we argue that there is an urgent need to align systems security and systems usability objectives for computer-based information systems. Further, in order to align the systems security and systems usability objectives, a thorough understanding of the system security and usability objectives is critical. Such a thorough understanding is necessary to effectively align the systems security and systems usability objectives and to integrate into the initial stages of systems development process. Alignment of systems security without compromising the systems usability would secure the information systems efficiently and effectively and would also enhance the overall usability of these information systems. An integrated systems development process with an accurate assessment of systems security and systems usability objectives would not only enhance systems security but also improve systems usability.

1.3 Research Scope

In general, human perspectives on any topic would involve personal constructs and cognitive beliefs, collectively known as values. Understanding system owners, developers and users perspectives involve the understanding the values of these stakeholders. As such, deciphering the personal constructs and cognitive beliefs of system owners, developers and users during the process of systems development is critical for the successful alignment of systems security and systems usability objectives. In order to align the system security and usability objectives of computer-based

information systems, thorough understanding of the security and usability objectives from system owners, developers and from users' perspective is very critical. Using Value Focused Thinking, Dhillon and Torkzadeh (2006) presented information system security objectives from the system security professionals' perspective and were validated by IS experts.

The primary goal of this research is to identify the information system usability objectives from system users' perspective using similar Value Focused Thinking approach adopted by Dhillon and Torkzadeh (2006). The end result of this analysis is systems usability objectives. After the identification of system usability objectives, this research compares the system security objectives identified by Dhillon & Torkzadeh (2006) with the system usability objectives and proposes an approach to align the system security and usability objectives by minimizing the impact of any conflicting security and usability objectives on the overall system security and system usability. To further elaborate, this research addresses the following research questions:

- What are the usability objectives from system users' perspectives?
- Which of the systems security and systems usability objectives are conflicting with each other and to what extent? How can an organization categorize and prioritize these systems security and systems usability objectives?
- Finally, how can these conflicting systems security and systems usability objectives be aligned to secure the information systems efficiently and effectively while ensuring user satisfaction?

From an information system theory, as well as practice stand point, the purpose of this research is to identify the usability objectives within the context of an information system

and align the security and usability objectives to provide system development design guidance for the software developers and engineers and information system owners. Such design development guidance may be developed for various levels of systems development process, which will be helpful for the software developers and engineers (Karat and Karat 2003).

The primary contribution of this research is a set of systems security and systems usability objectives that will help design a secure and usable computer based information system.

1.4 Dissertation Structure

The second chapter of this dissertation presents a review of existing literature in information systems security and usability. This chapter highlights the current research gaps within information system security and usability and how these two bodies of literature inform and support the primary argument of the thesis.

The third chapter of this dissertation discusses the theoretical and methodological assumptions that provide the basis for a detailed study of the elicitation of usability objectives and alignment of systems security and usability objectives without compromising on either the systems security or usability. In this chapter, we also present the Value Focused Thinking as a framework with which usability objectives are elicited from system users. Furthermore, this chapter discusses the analytical hierarchy process (AHP) concepts that will be utilized in this dissertation.

The fourth chapter discusses the data collection methodology and how and where the data collected was collected to understand the usability objectives from system users'

perspective. This chapter also analyzes the data collected through this research and presents the research results.

In the fifth chapter of this dissertation, the security objectives proposed by Dhillon and Torkzadeh (2006) and the usability requirements identified in this research are analyzed to identify any conflicting objectives and to arrange the security and usability objectives in hierarchies using Analytic Hierarchy Processing (AHP) concepts.

In chapter six, we analyze a case of computer hacking and identify which of the security and usability objectives that have not been met in that case study.

The seventh and final chapter of this dissertation concludes this research by discussing the theoretical, methodological and practical contributions of this research, research limitations and future research opportunities.

Chapter 2 – Literature Review

2.1 Introduction

The primary focus of this research is to align information security and usability objectives for computer based information systems. There is little research done to understand the system usability objectives from system users' perspectives. Moreover, the existing information systems research has not focused so far on how to align the information security and usability objectives. There is a common perception that security and usability are competing in nature and are mutually exclusive goals in that the higher the security of a computer based information system, the lower the usability of that system (Gunson, Marshall et al. 2011). In order to fully understand the research problem that is being addressed in this dissertation, a thorough understanding of the existing research issues in information security and information usability domains is necessary. The remainder of this chapter is divided into five main sections. Section 2.2 provides a framework for reviewing the security and usability literature domains, Section 2.3 provides a detailed overview of information system security literature, Section 2.4 provides an overview of information system usability literature, Section 2.5 links IT decision making with the existing state of security and usability research and Section 2.6 concludes the literature review.

2.2 Literature Review Framework

Information system security and usability concepts are essential ingredients throughout the system development life cycle. A review of the security and usability literature viewed through the lens of system development methodology provides a better understanding of the current research issues in these two domains. Any systems

development process that leads to the creation of useful organizational information systems uses accepted methodologies, techniques and tools (George, Batra et al. 2004). While a methodology is a step-by-step approach of how the various systems development phases are performed, the techniques and tools provide necessary support for the successful completion of the systems development phases. The systems development methodologies have been transforming over the last several decades to reflect the changing organizational preferences and increased technological capabilities and challenges.

A traditional systems development methodology consists of four primary phases, namely planning, analysis, development and testing and implementation. Each of these four phases consists of several sub-phases and other activities that must be completed in full for the overall successful completion of that particular phase.

The traditional structured systems development methods have been replaced with more sophisticated methods such as proto typing, objected oriented systems analysis, unified processes and agile methodologies. Each of these methodologies will have different variations of the four core systems development phases. For example, the waterfall method of systems development life cycle consists of project planning, requirements definition, design, development, integration, testing, installation and acceptance. In the waterfall method, the usual assumption is that all the phases of systems development will be performed in sequence or in a linear fashion. However, this assumption is not a valid assumption for all the systems development scenarios. Sometimes, some or all of these systems development phases are required to be performed in non-sequential or non-linear fashion to accommodate various practical issues of systems development an organization

typically encounters, such as continuous changes in requirements and changing scope of the project.

The real world's unique demands for development of information systems paved the way to several iterative systems development methodologies. In an iterative systems development methodology, some or all of the systems development phases are repeated in iterations until a perfect information systems is successfully developed and implemented.

One noteworthy iterative systems development methodology is unified process with industry standard diagramming notations. Unified process is a generic variation of IBM's Rational Unified Process, which has been used in IBM's Rational Rose Software. The unified process of systems development methodology will have four core phases, namely inception, elaboration, construction and transition (Larman 2005). Each of the four core phases will be repeated in iterations over the course of the project or until those phases are deemed to be unnecessary. Such an iterative approach of the systems development core phases is neither sequential nor linear. For each iteration, the systems development core phases will be implemented in an order that is suitable for the business scenarios and depending on the organizational requirements.

Irrespective of the nomenclature, categorizations, business environment in which the systems are developed or the available technological capabilities, it can be concluded that any information systems development effort must go through iterations/variations of all of the following four critical phases of information systems development:

- Analysis: This phase is defined as "formal modeling of the problem." However, it could also include the requirements analysis.

- Design: This phase is defined as "formalizing the transfer of domain knowledge." It also includes the construction of the actual system.
- Implementation: This phase is defined as "the transition or migration from the legacy systems to new system." The approach can be a top down approach used by management to implement the information systems.
- Adoption: User acceptability and adoption (includes resistance)

A brief description of the security and usability definitions are also mentioned here:

- Security: Information systems security includes confidentiality, integrity, availability, authentication and non-repudiation.
- Usability: Usability is the extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency, and satisfaction in a specified context of use.

Using the four critical systems development phases as a framework, we analyze the existing information systems security and usability literature streams. Relevant published scholarly research papers from security and usability research stream have been reviewed, analyzed and discussed in the following sections. Moreover, each relevant paper is categorized as belonging to one of the four critical phases of the information systems development methodology. See Table 2.1 below for a summary of the information systems security and usability literature streams, along with relevant scholarly papers.

Table 2.1: Summary of the Literature Review

	Analysis	Design	Implementation	Adoption
Security	(Pfleeger 1997; Dhillon and Backhouse 2001; Dhillon 2007);	(Boland 1978; Lane 1985; Baskerville 1993)	(Dhillon 1995; Dhillon 1997; Zurko and Simon 1997; Eloff and Eloff 2003; Smith and Frisby 2004; Bakke, Faley et al. 2005)	(Backhouse and Dhillon 1996; Baskerville and Siponen 2002; Harrison 2002; Cavalli, Mattasoglio et al. 2004; Furnell, Jusoh et al. 2005; Dhillon and Torkzadeh 2006)
Usability	(Darke and Shanks 1997; Schultz, Proctor et al. 2001)	(Adams and Sasse 1999; Palmer 2002)	(Adams and Sasse 1999; Whitten and Tygar 1999; Schultz, Proctor et al. 2001; Agarwal and Venkatesh 2002; Yee 2004)	(Whitten and Tygar 1998; Venkatesh 2000; Krauss 2003; Liimatainen 2005)

2.3 Security Literature Review

In this section, first we define the terms such as ”information system” and “information systems security” and discuss why information security is critical to organizations in general and to computer based information systems in particular. Then we delineate the predominant themes in information systems security literature. Furthermore, we discuss what and how this particular domain of literature informs the core argument of the thesis that there is an urgent need to align security and usability requirements for computer based information systems. Finally, we finally present summary and conclusions of information systems security literature review.

National Institute of Standards and Technology (NIST 2009) special publication 800-53 on Information Security defines Information System (IS) as a "discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of information." Ives, Hamilton et al. (1980, p.910) defines the term Management Information System (MIS) or more commonly known Information System (IS) as a "computer based organizational information system which provides information support for management activities and functions". Ives, Hamilton et al. (1980) further clarify that an information systems could be either transaction systems or management-oriented systems and any single sub-system or an application that is part of the overall information system could be called as Information Sub-System (ISS). As such, Ives, et al. present a broader view of the information system in an organization where an information system is a collection of several applications or sub-systems that support underlying business functions, whatever maybe such business function. Hence, for the purposes of this dissertation, the term Information System includes any application or system or sub-system that supports a business function.

Regarded by IT industry as the most comprehensive best practices framework, ISO/IEC 17799:2005 (Information Technology – Security Techniques – Code of Practice for Information Security Management) (ISO/IEC 2005) defines information security as "the preservation of information confidentiality, integrity and availability of information; in addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved " (Saint-Germain 2005). Ryan and Bordloi (1997) acknowledge that the goal of information security is to ensure the availability of information and information processing resources and to provide means to establish and

to retain the integrity and confidentiality of information within the system. Addressing information systems security using the attributes approach, Avizienis, Laprie et al. (2004) clarifies that security is "a composite of the attributes of confidentiality, integrity and availability, requiring the concurrent existence of 1) availability for authorized actions only, 2) confidentiality and 3) integrity with "improper" meaning "unauthorized"." Avizienis, Laprie et al. (2004) highlight that information security exists if and only if all of the three primary attributes of the information security are present, namely confidentiality, integrity and availability. Avizienis, Laprie et al. (2004) also describe the secondary attributes that are relevant for information system security which include accountability (availability and integrity of the identity of the person who performed an operation), authenticity (integrity of the message content and origin) and non-repudiability (availability and integrity of the sender and receivers of the message) Avizienis, Laprie et al. (2004, p.23). The three secondary attributes of the information systems security are derivatives of the primary attributes of the information security, namely confidentiality, integrity and availability.

As such, dubbed as the classical CIA approach, information security means confidentiality, integrity and availability of the data that is associated with an information system, which includes data security. However, information security contains not only data security elements, but several other security aspects. Information security includes business recovery plan, disaster recovery plan and emergency management plan.

In the late 1990s and during the internet dot com boom era, the topic of information systems security had gained a great deal of visibility due to the internet worms, virus strains and security issues in various tools and technologies (Pfleeger 1997). Pfleeger

argues that information systems security demands as much rigor, if not more, as other computing areas such as safety-critical-high-reliability applications (Pfleeger 1997, p.15). Since then, the advancement of information technology and proliferation of computers and mobile devices usage have only increased the continued importance of the information systems security. Organizations and individual spend several millions, if not billions, of dollars to protect their organizational and personal computer systems from unwanted information security threats.

ISO/IEC 17799:2005 (Information Technology – Security Techniques – Code of Practice for Information Security Management) (ISO/IEC 2005) also dwells deeply on why information security is needed and notes that information, supporting processes, systems and networks are critical business assets and protecting these critical assets is essential to maintain "competitive edge, cash flow, profitability, legal compliance and commercial image." This statement sums up the need for information security in any type of organizational environment as many organizations today are increasing their IT spending to manage competition, enhance cash flows and profitability, maximize compliance and minimize any damage to the reputation.

Information security has several themes. Depending on how the analysis was performed, information systems security can take any number of themes. As pointed out by Dhillon (2004), there are several issues to be considered to ensure adequate information systems security. These issues include understanding what is meant by information system security, enhancing the non-technical orientation to information security controls, enforcement of information security policies and understanding the behavioral and social aspects of an organization. Dhillon (2004) highlights that "understanding the social

processes and ways in which people communicate with each other determine information security."

Part of the information system security research highlights the themes of senior management's decision making and security policy formulation aspects as a mechanism to pave the way for proactive management of organizational information security. This research loosely corresponds to the analysis and design phases of the systems development.

The information security function in any business sector defines the safeguards for security based on the knowledge of security requirements and the potential threats to the information assets (Cavalli, Mattasoglio et al. 2004). Traditionally, security of computer based information systems is concerned with the methods of providing cost effective and operationally effective protection of information systems from undesirable future events or threats (Lane 1985). For purposes of this research, we adopt the definition of information systems security that coincides with the definition of information systems with three sub-systems namely, formal, informal and technical.

Information systems security is a critical issue for the technical sub-system of the information systems. According to Dhillon (2007), given the nature of the technical sub-systems, the security of such systems equates to the maintenance of confidentiality, integrity, availability, authentication and non-repudiation. Such a broad view of information systems security matches the contemporary concept known as Information Assurance. This is because information assurance also consists of five system attributes that are designed to characterize the ability of the system to protect and defend information and information system (Bail 2006). And these attributes of information

systems security include confidentiality, integrity, availability, authentication and non-repudiation (Bail, 2006). Information assurance integrates all the classical elements of the definition of information systems security, confidentiality, integrity and availability. Information security has been one of the single most critical issues ever since organizations started using information systems to conduct their business operations. The criminology theory of General Deterrence assumes that potential violators become aware of the efforts to control anti-social behaviors (Straub 1990). This underlying assumption motivates the internal users not to commit any type of computer abuse. Using the criminology theory of general deterrence, Straub (1990) investigates "*whether a management decision to invest in information systems security results in more effective control of computer abuse*" and proposes that deterrence measures must include certainty and severity of sanctions against computer abuse. Straub (1990) also points out that low managerial interest in security stems from the strong managerial belief that information systems security is inherent in the industry and that the general risk mitigation measures taken to protect the information systems are sufficient. However, Straub (1990) makes a clear distinction between the risk management and management of risk and makes a strong case that management has to understand the difference between these two concepts which would help the managers to make key decisions about the information security function.

Further, Straub (1990) also indicated that effective deterrence security measures decrease the intentional computer abuse from the internal users. Organizations must formulate these deterrent security measures at various levels including organizational, corporate level and lower level highlighting the strategic, tactical and operational aspects of the

security policies. Formulation and communication of these policies act as a severe deterrent to the users of information systems. Dhillon and Backhouse (2001) and Dhillon and Torkzadeh (2006) also highlight that organizations must have a computer security strategy which would provide the guidelines to the lower level managers to formulate the policies. Baskerville (1993) argues that the emergent organizations need a meta-policy about security policies which will help ensure and modify the security policies.

Another major theme in information security literature is security risk assessment, which also corresponds to the analysis and design phases of the systems development. Risk is a function of the environment in which the risks are perceived. Risk analysis is the process of identification of risks while the risk management determines the degree of exposure (Backhouse and Dhillon 1996). Risk assessment, consisting of risk analysis and risk management, is also an active process that is used to evaluate the security of an IT environment (Backhouse and Dhillon 1996). In their case study in a provincial multi-specialty hospital, Cavalli, Mattasoglio et al. (2004) argue that providing information security requires some serious risk analysis/risk assessment. They present that after a thorough risk analysis, the management has one of the four choices: accepting the risk, avoiding the risk, reducing the risk or transferring the risk. This process calls for decision making choices for the management and links to the prior theme discussed in the following Section 2.5.

One other theme in information security research that draws researchers' attention is the effectiveness of security and several ways to measure the information security effectiveness. This theme corresponds to the implementation and adoption phases of systems development. According to Kankanhalli, Teo et al. (2003), organizations are

reluctant to spend resources on enhancing IS security due to the nature of security threats and lack of understanding the IS security effectiveness (Kankanhalli, Teo et al. 2003). Organizations tend to be reactive as opposed to be proactive to prevent any losses arising out of the information security threats. Kankanhalli, Teo et al. (2003) also attest that there is a huge research gap between theoretically tested models and empirically tested models. In their study, authors propose an integrative model of IS security effectiveness and empirically test the model. The empirical model incorporates critical organizational factors such as organizational size, top management support and industry type.

Addressing a different variation of information security, Segev and Porra (1998), in a case study, highlight two critical points for the Internet security. Firstly, implementing technical solutions is not enough to ensure Internet security. Secondly, Internet security, just like information systems security, requires top management attention and resources. This case study illustrates that Internet security be treated as corporate level security issue rather than a local technology issue.

Eloff and Eloff (2003) propose an Information Security Management System (ISMS) framework to facilitate a relationship between information security processes and products. Accordingly, by intelligently mixing an appropriate combination of policies, standards, procedures, codes-of-practice, technology and human, legal and ethical issues, authors argue that organizations can secure the information and technology related assets. ISMS consists of product as one of the components of the frame work. However, this component has not been elaborated significantly to include various issues that affect the security technologies. Finding the right balance between the usability of such security

technologies and mechanisms is a critical aspect to ensure the overall security of the organizational information and technology assets.

In discussing the information security concepts and practices within the healthcare industry, Cavalli, Mattasoglio et al. (2004) highlight several information system security concepts that resonate across all industries. Cavalli, Mattasoglio et al. (2004), using the case of a provincial multi-specialty hospital in Italy, note that information systems security is a complex topic and an organization can only define the safeguards for information system security based on the knowledge of security requirements. These authors propose security requirements that are specific to health care organization that operate in Italy. By extending this argument to industries outside healthcare where the need to for information system security is ever increasing, we argue that understanding and defining security requirements are critical to ensuring the information system security.

Leach (2003) postulates that the internal security threats from the existing or past employees are due to poor user security behavior as 80% of major security failures could be the result of inappropriate security options in computer based information systems. Leach (2003) notes that since the employees modulate their security behaviors according to the values and attitudes demonstrated by the senior management, it is highly crucial for an organization to carefully influence the users' security behavior to drive down the level and severity of the security incidents.

In summary, security is a key component of any computer based information system and protecting the confidentiality, integrity and availability of the system components and data is critical for any organization to survive in the global competitive world.

2.4 Usability Literature Review

In this section, we first define the term "usability" and discuss why it is significant to organizations in general and to computer based information systems in particular. We then outline the significant themes in usability literature. Additionally, we discuss what and how this particular body of usability literature informs the argument of the thesis that there is an urgent need to align security and usability requirements for computer based information systems. Finally, we present summary and conclusions of usability literature review.

National Institute of Standards and Technology (NIST 2009) special publication 800-53 on Information Security defines the term "user" as an "individual, or (system) process acting on behalf of an individual, authorized to access an information system." To put it in more common parlance, the term "user" refers to the "individual who is accountable for some identifiable set of activities in a computer system" (Saltzer and Schroeder 1975). Ever since computer based information systems gained prominence in human lives, the concept of usability has been lingering both in academic and practioners' world. Melone (1990) proved that users develop negative attitude toward a system if they find it difficult to use. In a study to identify and assess the relative importance of overall customer satisfaction for software products and service support, Kekre, Krishnan et al. (1995) conclude that usability is one of the critical drivers for customer satisfaction. However, usability in this context is more viewed from the perspective of "interface design" as opposed to the modern perspective of "task-driven."

International Standards Organization (ISO) defines the term "usability" as "the extent to which a product can be used by specified users to achieve specified goals with

effectiveness, efficiency and satisfaction in a specified context of use" (ISO 1998). Even though there are several definitions and descriptions of the term "usability", the ISO's definition of usability seems to be the most appropriate for this research as the definition focuses on the context in which information system is used and the efficiency, effectiveness and satisfaction are dependent on such contextual use.

In general, "usability" can be described as the ability of the users to navigate and perform the intended functions within a system. Widely accepted and prominent information security standards such as ISO 17799 provide an authoritative statement on information security and the procedures to be adopted by organizations to ensure information security (Ma and Pearson 2005). International Standards Organization defines the term system usability as the ability of the system performs specific goals in a particular environment with efficiency, effectiveness and satisfaction (ISO 1998). However, there are few standards or guidelines for usability and accessibility of information systems. Currently, there are no mechanisms to understand and interpret what users value the most. Whether it is a computer based information system or web applications, appropriate information systems security and usability measures must be put in place. The usability and accessibility research has largely focused on the web front end and not much research has been conducted to understand the impact and influence of individual values on the usability and accessibility of the information system.

DiAngelo and Petrun (1995), noting that accurate definition and assessment of customers' (also known as low-level audiences such as software implementers, end users and technical decision makers) needs and wants form the basis of software products that emphasize usability, propose a requirements-gathering methodology that focuses on

usability and user requirements. DiAngelo and Petrun (1995) conclude that the term usability focuses on "user tasks and satisfaction." During the initial software development days, usability is synonymous to software products that let users do what they want do. Gunson, Marshall et al. (2011) investigated the user (banking customers) perceptions of the usability and security by comparing two different security authentication mechanisms, namely single-factor and two-factor authentications. As noted in their research conclusions, the security gains of having additional factor of authentication were off-set by the lower user perceptions of usability.

Various published articles on the topic of usability as they relate can be typically categorized into two categories namely, usability and usable security articles. Usability literature includes scholarly papers such as Schultz, Proctor et al. (2001), in which authors highlight that little research has been conducted on the usability issues associated with information security methods. They indicate that usability is a critical factor in users' willingness to maintain security and highlight the need for HCI researchers to focus their efforts on systematic investigation of usability issues associated with information security related tasks.

Research on usability also discusses various aspects of usability testing. In one particular scenario, Krauss (2003) highlights that usability is synonymous with the ease of use. He further indicates that "in a usability test, tasks are again attempted but, unlike a design walk-through, functioning code is used, and participants are asked to actually perform tasks on their own while their interaction is observed, their comments are recorded, and usability problems are noted for subsequent causal analysis (Krauss 2003, p. 584)." The core argument Krauss makes is that since technology is being used by the end-users

remotely, any usability testing must engage in remote testing to accurately understand the issues involved in remote usage situation. Currently, there is little usability testing on the remote usage of technology.

Another usability research stream suggests using various techniques to improve the usability of various security mechanisms. For example, Ratha, Connell et al. (2001) discuss several methods to enhance the security and privacy in biometric-based authentication systems. In their discussion, they observe that "simply extending the length of passwords to get equivalent bit strength presents significant usability problems (Ratha, Connell et al. 2001, p. 615)." They also argue that "biometrics-based authentication has many usability advantages over traditional systems such as passwords (Ratha, Connell et al. 2001, p. 633)."

Another stream of usability literature, as it relates to information security, can be termed as usable security literature, which deals with usable security or usability of security features in end-user software. In their examination of possible usability challenges posed by security features in end-user software such as Internet Explorer, Outlook Express and Word, Furnell, Jusho et al. (2005) conclude that users still face "significant impediments" when it comes to security features in end-user software. These authors conclude that given the security and usability problems that end-users encounter, majority of the end-users will either misuse or mis-configure the security options and features.

"The impact of technology developments such as pervasive computing and the Internet have led to an increased examination of human issues such as privacy, trust, and security (Karat and Karat 2003, p. 533)" (emphasis added). They also summarize that the ISO

9241 standard, especially parts 10 and 11 significantly acknowledge that “usability is complex and context dependent (Karat and Karat 2003, p. 535).”

In their research paper on user perceptions of security and usability of various security authentication mechanisms in banking industry, Gunson, Marshall et al. (2011) address certain gaps in the usability and security. Gunson, Marshall et al. (2011) test the differences between two authentication methods in terms of perceived usability by the end users and conclude that users perceived that the less-complex authentication process was found to be significantly more usable than the more-complex authentication process. In addition, these authors also found that users ranked the less-complex authentication process as the most convenient by a significant margin since the mechanism is easier to use (Gunson, Marshall et al. 2011). Similarly, Weir, Douglas et al. (2009) also compared the three different security authentication devices and found that users chose the device that they perceived the least secure.

Flechais, Sasse et al. (2003) underscore the importance of developers play a key role in the provision of usable and effective security for computer based information systems. Flechais, Sasse et al. (2003) also present a methodology to enhance the usability of security. The point that is critical for the current thesis from the above discussion is that usability can be as simple as having appropriate design and features that are well received in the real world by the end users and developers alike.

In summary, usability, usable security and secure usability are all critical for a computer based information system to be secure and to be usable and to meet the goals of the organization as well as other IT stakeholders.

2.5 Discussion

Decision Making in IT

As noted in the previous section, managing information systems security and usability involves several decision-making choices by the system owners, users and developers, (collectively known as IT stakeholders). These stakeholders make several decisions about security and usability either during various stages of the system development life cycle stages or during the intended use of an information system. In this connection, it is only critical to understand the decision making in IT in general and factors that influence the decision-making behavior of the above IT stakeholders in particular because Sharda, Barr et al. (1988) notes that the value of an information system is tied, among other things, to constraints on design effectiveness.

IT in the form of "Management Information Systems provides for the information necessary to support the purposeful behaviors of the managers (Henderson and West Jr. 1979)." One positive consequence of using IT by the managers in organizations is in the areas of decision-making. As discussed by Power (1983), decision activities and decision structures have radically been altered by the use of information provided by IT.

Decision making in IT comprises several dimensions. These include, but are not limited to, decision-making for investment in IT, decision making for planning IT within an organization, decision making for changes in organizational structure that would enable effective use of IT and selection of various IT security and usability alternatives.

Finding a common ground among IT stakeholders involved in making choices for security and usability is critical for better decision-making outcomes. As noted by Davenport (2009) decision-making involves avoiding several pitfalls including "group think" phenomenon. Davenport (2009) suggests that smart organizations can improve

decision-making by identifying the most important decisions to be made, inventorying factors that go into these important decisions, designing a broad and inclusive decision-making approach and institutionalizing the entire decision-making process. Davenport (2009) also argues that use of information technology either in the form of "Analytics" or in the form of "Automation" must be balanced with human intuition and judgment. He states that managers should not incorporate business analytical models or assumptions they do not understand.

Davenport, Hammer et al. (1989) argue that the key to effective decision-making process is to gather a handful of people who deeply understand either the business or the technology and who are committed to the process. In the case of choices for IT security and usability, the IT stakeholders have the necessary technical and business knowledge and have the motivation to make appropriate choices for IT security and usability as these IT stakeholders realize that their choices will make or break the implementation and successful usage of the IT.

Debrabander and Edstrom (1977), by studying the communication patters of IS specialists and users, concluded that conflicts exist between IS specialists and users because they bring different perspectives to their interactions. Understanding the perspectives that system owners, users and developers bring to the system development life cycle in general and to the application of IT security and usability in particular is critical for the alignment of IT security and usability.

Debrabander and Edstrom (1977) argue that the interaction between system users and system specialists (*such as system owners and system developers*) is expected to increase the quality of the final outcome of the systems development. Debrabander and Edstrom

propose a theoretical framework that recognizes the factors that govern effective communication among the system uses and system specialists. According to Debrabander and Edstrom's theoretical framework, the interaction process between a potential user and a system design specialist is a dyadic relationship, which can develop into mere exchange of information, use of side payments or the application of punishment (Debrabander and Edstrom 1977). The final outcome of the dyadic relationship depends on the setting and type of relationship that exists between the potential system users and the system specialists.

The typical relationship between system users and system owners/system developers is formal in an organizational setting. Under such formal circumstances in an organization, the final outcome of the interaction between system users and system owners/developers are the perceptions of IT security and usability.

Other research examining the Chief Information Officers' (CIOs) decision making authority conclude that CIOs decision making authority is influenced by several factors including organizational climate, organizational support of IT, CIO's structural power, CIO's personal level of strategic effectiveness and partnership and support of top management team (Preston and Chen 2008). However, these conclusions are based on the theoretical posture of power and politics and managerial discretion.

Another stream of research focuses on the IT investment decisions that senior IT leadership engages constantly in any organizational setting and how this process is managed. Typically, decision making requires prior knowledge of information relating to the decision situations. Rose, Rose et al. (2004) noted that when the IT investment decisions are evaluated in a port-mortem analysis, it happens that the personal risk

preferences of the decision evaluators may lead to a biased evaluation of the IT investment decision out comes. Similarly, Angelou and Economides (2008) propose a quantitative model called Real Options (ROs) analysis for valuating Information and Communication Technologies (ICT) infrastructure investments. As noted by the authors, the RO analysis for evaluating ICT infrastructure investments is difficult to implement in situations where the decision variables cannot be quantified or where the decision variables are qualitative in nature.

As shown in above paragraphs, it is evident that understanding how IT stakeholders approach the topics of information system security and usability is critical for the alignment of information security and usability. The factors that influence IT stakeholders' for making several security and usability decisions during the development, implementation and on-going usage of the information systems are critical for ensuring that information systems are developed in consistent with the expectations of the key IT stakeholders.

Security and Usability

Typically, in any discussion of security and usability issues, users are the first to be blamed for being the weakest link and less motivated to adopt any stringent security measures. On the contrary, Adams and Sasse (1999) recognized the importance of challenging the view that "users are never motivated to behave in a secure manner." Adams and Sasse (1999) affirm that user apathy toward not behaving in a secure manner is due to lack of user-centered design in security mechanisms. Adams and Sasse (1999) claim that the usability of most commonly used security mechanism such as passwords, has been rarely investigated.

Hoffman, Grivel et al. (2005) argue that "some architecture decisions may unknowingly limit the ability to implement usability requirements" (Hoffman, Grivel et al. 2005, p. 469). Therefore, it is clear that security is one of the information systems architectural decisions that IT executives focus leaving critical system usability decisions unaddressed. Liimatainen (2005), in a study to search for usability problems of decentralized authorization systems, identifies various usability problems within systems security context and they include "authorization of entities, definition of a security policy for a resource, revocation of rights, checking validity of a set of credentials, privacy of users, and distinguishing trusted channels. Whitten and Tyger (1999) present that a security system is usable if, apart from other aspects, its users are aware of the security risks and know how to perform the necessary tasks. Johnston, Eloff et al. (2003) highlight the seemingly diverse goals of information security and human computer interaction. For example, the implementation of the most common security mechanism, such as passwords, needs to consider the appropriately between security and usability. Otherwise, end-users tend to write down the passwords on notes, which completely make all the organizational policies and procedures null and void. Johnston, Eloff et al. (2003) also point out that "even the most user-friendly interface could be avoided by users unless there are policies in place which enforce the use of security programs (Johnston, Eloff et al. 2003, p. 684)."

As noted in the above paragraphs, system security and system usability are core elements in the development of computer based information systems. In their detailed analysis of existing information systems and security research, Dhillon and Backhouse (2001) use four paradigms, namely functionalist, interpretive, radical humanist and radical

structuralist, to identify the gaps in the information systems and security research. As noted by the authors, traditional risk analysis and security evaluation methods fall into functionalist paradigm that provide practical solutions to practical problems. Dhillon and Backhouse (2001) conclude that the overall security can be achieved by analyzing the behavior of constituent elements of the system. We extend this argument to postulate the core argument for this thesis in that understanding the security and usability from the perspectives of system security professionals and system users respectively is critical for the successful development, implementation and usage of computer based information systems.

As such, Dhillon & Torkzadeh (2006) used the Value Focused Thinking approach to explore and understand information system security in terms of the values of the people such as security professionals. Dhillon and Torkzadeh (2006) proposed a set of information system security objectives. Similarly, understanding the information systems usability from the perspective of the information system users and developing information system usability objectives is critical to align the security and usability objectives.

2.6 Conclusions

As discussed above, system security and system usability of computer based information systems can be immensely improved by defining the usability objectives and leveraging the existing security objectives developed by Dhillon and Torkzadeh (2006). Casting choices made by the IT stakeholders during the course of systems development process for information system security and usability as the decision making choices and defining

and aligning the security and usability objectives paves the way for better development of computer based information systems.

In addition, the system security depends on the actions undertaken by the users and system administrators. Studying the existing security and usability objectives and their implementation will reveal the existing gaps and deficiencies for better security and usability. The main idea of this research is to understand the security and usability objectives within an information system and present them as design guidance for the software developers and engineers. Such design development guidance may be developed at various levels which will be helpful for the software developers and engineers (Karat and Karat 2003).

Chapter 3 - Research Methodology

3.1 Introduction

The purpose of this chapter is to discuss the theoretical and methodological assumptions that provide the basis for a detailed study to align the security and usability objectives of computer based information systems. As outlined in the previous chapter, the existing literature establishes that information system stakeholders (such as system security professionals, system developers, system owners and system users) are continually put in decision making situations. In such decision making situations, these stakeholders have to express their preferences by choosing among several alternatives of system security and system usability features during their interactions with the computer based information systems. As noted by Catton (1952), the preferences expressed by individuals in any given situation are not random but patterned and these patterns are governed by the underlying values of the individuals who express the preferences. Hence, in order to better align the security and usability objectives of a computer based information system, it is critical to understand the values of system stakeholders. A thorough understanding of what the system stakeholders really value in a given system security and usability context provides a better opportunity to align the system security and usability objectives.

There are several ways to assess and understand values. Value-focused thinking (VFT) is one of several approaches that have been popular in information systems research (Dhillon and Torkzadeh 2006; Mishra 2008; Harris 2010) VFT can be used to understand the values that influence the decision makers in decision making situations. VFT helps in clearly defining and structuring the fundamental values in terms of objectives and use

these objectives to help guide the decision making situation (Keeney 1994). Dhillon & Torkzadeh (2006) used the VFT to assess the security values of 103 information security professionals and to define the information system security objectives.

In this research, we use VFT approach to assess the usability values of independent information system users and developers and to define the information system usability objectives. After such an assessment of the usability objectives, we then compare those to the information system security objectives proposed by Dhillon and Torkzadeh (2006) using Analytical Hierarchy Process (AHP) and align the security and usability objectives. The next section provides an overview of VFT approach and how this approach is used in information systems research. The following section discusses the AHP and how this concept is used to compare the security and usability objectives. The next two sections present the research design for data collection and the final section provides conclusions for this chapter.

3.2 Value-Focused Thinking

Typically, a decision maker analyzes the alternatives available within the decision making problem domain and chooses those alternatives that are expected to achieve the intended objectives. However, more often than not, such alternatives chosen do not meet the required objectives that the decision maker has in mind. Depending on the circumstances, the reasons for not achieving the original objective the decision maker had in mind could be several including the fact that the decisions made by one decision maker with a particular objective in mind are perhaps in direct conflict with the objectives another decision maker has in mind. For example, a system developer, with a limited understanding of what a system user really cares about while using computer based

information system, is faced with the challenge to incorporate several system security and usability features. If the system developer chooses a particular alternative of either security or usability feature that the ultimate system user does not value, the so-called system security or usability feature chosen by the system developer is rendered useless. The fundamental problem in this given example is that the decision maker, faced with a decision, chooses among the various alternatives that are plausible to a given decision making situation without any understanding of the real objectives. Keeney (1992) argues that such a decision making approach is not pro-active and identifies the decision alternatives prior to the identification of values, which is truly what a decision maker cares about. Keeney (1992) instead proposed Value Focused Thinking (VFT) approach, which can be used in various decision making situations by starting with the values a decision maker truly cares about and structuring those values in terms of objectives to help guide the decision making process. If a decision maker is only focused on choosing one or more of the several alternatives available for a particular situation, the decision outcome is restricted to the alternatives already pre-identified for the given decision situation. These pre-defined alternatives may or may not be consistent with the values of the individuals involved in the decision making situation. Information system security and usability involves various stakeholders in various stages of the development of computer based information system. These stakeholders, as it relates to the security and usability of a system, include but are not limited to, system developers, users and owners. Keeney (1992) proposes that, by focusing early and deeply on the values, the decision making situation provides more desirable consequences. What this means for security and usability of an information system is that a thorough understanding values of the

stakeholders at early stages of the system development process helps with the alignment of security and usability objectives of the information systems.

Values are principles used for evaluating the desirability of any possible alternatives of any given situation (Keeney 1992; Keeney 1994). Individuals evaluating any type of situation that they encounter in their daily or professional life use their respective personal values as a basis or framework for evaluation of the situation, act up on it and make appropriate decisions, if decisive action is warranted. Moreover, Keeney points that understanding "the values relevant to a given situation indicate what information is important" (Keeney 1992, p. 24). In order to really minimize the conflicting choices made by the system stakeholders in the realm of security and usability that would compromise the overall objective of enhancing the system security and system usability, understanding the system stakeholders' values is critical.

For information system security and usability, the information system stakeholders (such as system security professionals, system developers, system users, system owners, etc.) are constantly having to choose among various pre-defined choices of security and usability features, configurations, alternatives, etc. We argue that these pre-defined alternatives are inconsistent with the values of the information system stakeholders. Keeney notes that by "systematically appraising how well we are doing in terms of our values may suggest fruitful decision opportunities to formulate and pursue" (Keeney 1992, p.27). Hence, we propose that understanding the security and usability values of system stakeholders uncovers the security and usability objectives that the stakeholders really care about. By focusing on the security and usability objectives that stakeholders

really care about, we argue that information system security and usability can be enhanced.

Dhillon and Torkzadeh (2006) used VFT approach to interview and elicit the values of system security professionals to understand their values and proposed the system security objectives. In this dissertation, we argue that it is highly critical to formulate the usability objectives based on the values of the information system developers and users. Such an assessment of usability objectives based on values would present the stakeholders an opportunity to start with a clean slate and identify what they really want in system usability, rather than choosing among the usability alternatives that are marginally suitable either to the organization or available in an application development environment.

Keeney asserts that, in general, VFT is applicable to decision situations that are based on real decisions, that result in very important decisions to the person or the organization facing it and that each is a complex decision with no clear "solution" (Keeney 1992, p.22). He further notes that in order to solve a public problem involving various stakeholders, also known as decision makers, it is appropriate to start understanding their values because values are what many of the problem stakeholders are more familiar with and have view points and opinions.

As outlined in the literature review chapter, information security and usability decision making situations that system stakeholders encounter meet the above three characteristics. For example, when a system user encounters a typical situation where he or she has to choose the different alternatives and options of security and usability, such decisions are real decisions and are critical to the system users and the organizations to

which the system users belong to. In addition, each of these decisions made by the system users is complex in nature and there is no right or wrong answer.

By applying the VFT to understand the usability objectives, we argue that, similar to the security objectives identified by Dhillon and Torkzadeh (2006), appropriate usability objectives could be identified by focusing and understanding the values of the system developers and users.

At a high level, Keeney (1992) illustrates what it means to think about values and highlights the central role of "hard thinking" in VFT in the following diagram:

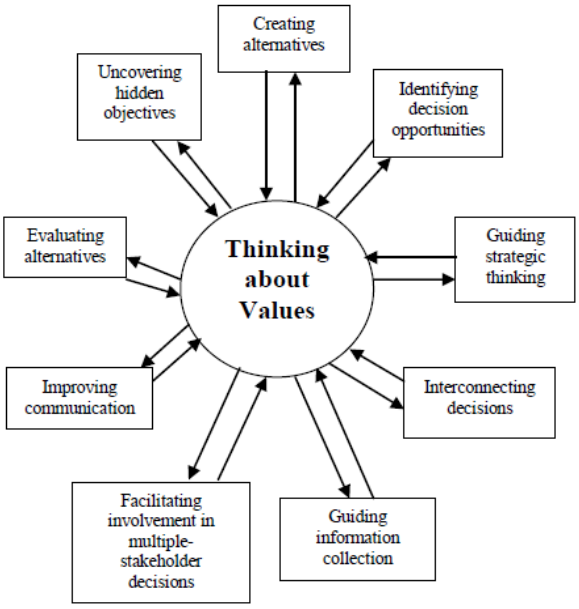


Figure 3.1: Overview of valued-focused thinking

Source: Keeney (1992, p.24)

As shown in the above diagram, thinking about values is central and critical to the VFT approach. Thinking and identifying values can be done by having discussions with the appropriate decision stakeholders. By having in-depth discussions with multiple stakeholders in the form of unstructured and open-ended interviews can be helpful to identify the values that these stakeholders care and feel near and dear. Keeney (1994)

argues that such discussions with multiple stakeholders could possibly result in a list of values, constraints, alternatives and criteria to evaluate alternatives that are redundant in nature. However, Keeney (1994) stresses that VFT with built-in redundancy provides complete and accurate list of values that a specific group of stakeholders really value and care about.

According to Keeney (1992; 1994) and Dhillon & Torkzadeh (2006), eliciting values from a group of stakeholders involved in a group decision making situation consists of the following steps:

- Having a discussion with relevant decision makers and stakeholders to elicit raw values;
- Cleaning up the raw values to make them more readable;
- Converting the cleaned up raw values into common form values by adding additional language to clarify any ambiguities without losing the original gist of the raw values expressed by the stakeholders;
- Converting the common form values into objectives and categorizing and distinguishing the fundamental and means objectives.

Keeney (1992; 1994) defines that an objective as a "statement of something one wants to strive toward." He further elaborates that an objective must possess three characteristic features namely, decision context, an object and a directional preference (Keeney 1994). For example, "Minimize access control" is one of the fundamental objectives identified by Dhillon & Torkzadeh (2006) in their value-focused assessment of information system security in organizations. The decision context is to maximize the IS security and the

objective in this particular example is access control with a directional preference of minimizing.

After identifying objectives, Keeney (1992; 1994) provides a conceptual basis to categorize the objectives in to fundamental objectives and means objectives by performing a "Why Is This Important?" (WITI) test. By deeply thinking about why each objective is important and finding the theoretical relationships among the objectives, the researcher can categorize the objectives into fundamental and means objectives. Keeney (1994) stresses that key element that would help this categorization is a clear understanding of how a particular objectives influences another objective.

Application of the above discussed approach by engaging with the system developers and users would result in usability values that system developers and users really care about. We argue that application of VFT to understand the usability values from stakeholders truly provides a different perspective to system usability. By leveraging the advantages attributed to the VFT methodology discussed by Keeney (1994), this research can uncover the hidden objectives and values of system developers and users within the system usability context and facilitates the participation of multiple stakeholders in the generation of decision alternatives that are critical for the system usability decision context.

3.3 Analytic Hierarchy Processing

As discussed previously, aligning the security and usability objectives in a computer based information system involves eliciting and understanding the values of system stakeholders using VFT. However, understanding the stakeholder values only helps bring the necessary objectives of security and usability that the system stakeholders really value. Aligning of system security and system usability objectives involves structuring and prioritizing these objectives into a hierarchy to zero in on the most important objectives of system security and usability that would achieve the overall objectives involved in building a computer based information system. In order to align the multiple objectives of system security and system usability, an appropriate method is necessary to structure and organize the security and usability objectives into a hierarchy. For this purpose, we propose the use of Analytic Hierarchy Processing (AHP). In the following paragraphs, we argue why AHP is the appropriate method to structure the conflicting objectives of security and usability into hierarchies.

AHP is a multi-criteria decision making tool in which various factors are arranged in a hierarchical structure (Saaty 1980; Saaty 1990). Security and usability objectives gathered from the system stakeholders are subjective expressions of preferences of what the stakeholders value in a given decision context. As with any multi-decision making situation, the primary challenge is to convert the subjective assessment of preferences into an objective measurement for further analysis. According Saaty (2001), AHP provides the "objective mathematics to process the inescapably subjective and personal preferences of an individual or a group making a decision" (Saaty 2001, p. 305).

In this research, we gathered the security and usability objectives based on the subjective values expressed by the system stakeholders and these values are all on different scales of preference of the individuals. The goal of this research is to appropriately interpret these objectives and the values underlying these objectives for the final alignment and to identify conflicting security and usability objectives. In order to achieve this goal, we use AHP which helps in the process of prioritization "by solving the problem of having to deal with different types of scales by interpreting their significance to the values of the user or users" (Saaty 2001, p. 305). AHP processes the inputs of subjective multi-dimensional units with different scales and transforms them into an objective uni-dimensional unit with a uniform scale for comparisons and for further analysis in a decision making situation.

Simply put, AHP involves three steps: state the objective, define the criteria and select the alternatives (Saaty 1990). The objective is the overall goal that is being accomplished. For example, within the current research, an overall goal or objective could be the minimizing the system security or maximizing the system usability. Criteria act as the lens to analyze the alternatives available in a given decision situation. Completing the above AHP three steps create a hierarchy for a decision making situation. Even though each hierarchy will have an overall objective and criterion related to the alternatives available, Saaty (1990) argues that hierarchy does not need to be complete with all the different levels for each decision making situation. Depending on the decision context, a particular criterion may or may not have a direct relation to a particular alternative. In order to develop hierarchies using AHP, Saaty (2001) proposed seven principles that provide guidance and these are briefly discussed below:

1. Ratio scales, proportionality and normalized ration scales are critical to the generation and synthesis of priorities (Saaty 2001, p. 306).

2. Reciprocal paired comparisons are used to express the judgments semantically linking them to a numerical fundamental scale of absolute numbers (Saaty 2001, p. 306) to arrive at the rankings of the alternatives in any one of the three modes, namely, relative, absolute or benchmarking. Alternatives are excluded in pair wise comparisons for relative measurement where as alternatives are also included in pair wise comparison for absolute measurement. Benchmarking uses one of the known alternatives in the group as a bench mark to compare other alternatives against it.

3. Sensitivity of the principal right eigenvector to perturbation in judgments limits the number of elements in each set of comparisons to a few and requires that they be homogeneous (Saaty 2001, p. 307).

4. Homogeneity and clustering are used to extend the fundamental scale gradually from cluster to adjacent cluster (Saaty 2001, p. 308).

5. Synthesis that can be extended to dependence and feedback is applied to the derived ration scales to create a uni-dimensional ration scales for representing the overall outcome (Saaty 2001, p. 308).

6. Rank preservation and reversal can be shown to occur without adding or deleting criteria (Saaty 2001, p. 308).

7. Group judgments must be integrated one at a time carefully and mathematically (Saaty 2001, p. 309).

We propose using the above principles and the other concepts of AHP to objectively prioritize the system security and system usability objectives derived from subjective values of system stakeholders.

3.4 Research Design

We believe that the appropriate research methodology to understand the personal values of the system owners, system developers and system users is an interpretive field study using VFT techniques. As pointed out by Klein and Myers (1999), "interpretive research can help IS researchers to understand human thought and action in a social and organizational contexts; it has the potential to produce deep insights into information systems phenomena and information systems development." The thoughts and actions of system developers and users are based on the personal values and these personal values are critical for mitigating risks associated with the security and usability of information systems. For the purposes of this thesis's scope, system owners are considered as the organization or the organizations that own the computer based information system and employ the system developers and users. Understanding the values of organizations is considered out of scope for this dissertation.

Understanding and capturing the personal values of system developers and system users within an organizational context preserves the nativity and originality of these values, which enables us to come to appropriate conclusions about the security and usability of information systems developed in the organizational context.

Generally speaking, the interpretive field studies include in-depth case studies and ethnographies (Klien and Myers 1999). Dhillon & Torkzadeh (2006) conducted a value-focused assessment of information system security in organizations by performing in-

depth interviews of system security professionals to elicit their values on system security and convert their values as security objectives using VFT techniques. We propose to follow similar approach to elicit the values of relevant stakeholders about the system usability and convert these values into system security objectives using VFT techniques. As such, for the purpose of this study, we propose to conduct in-depth interviews of system users to elicit the values that are important for them within the context of system usability. We will collect data regarding values by interviewing system developers and system users. The research participants belong to various organizations across the United States and all these research participants are heavily involved in various stages of systems development and system usage in their respective organizations.

As discussed in Dhillon & Torkzadeh (2006) value-focused assessment of information system security in organizations, data collection and analysis using VFT involves multiple steps and multiple iterations of some of these steps. Using a similar approach followed by Dhillon & Torkzadeh (2006) for system security objectives, data collection and analysis for the identification of information system usability objectives from information system developers' and users' perspective involves the following distinct processes and sub-processes:

1. Interviews:
    a. Eliciting "raw usability values" from research participants; and
    b. Converting "raw usability values" into "cleaned up usability values;"
2. Common Form Usability Values:
    a. "Cleaned up usability values" are converted into "common form usability values;"

b. Duplicate or redundant "common form usability values" are eliminated or merged;

c. Unique "common form usability values" are converted into "usability sub-objectives;" and

d. Based on similarity, "usability sub-objectives" are clustered and labeled as "usability objectives;"

3. Information System Usability Objectives:

a. Why Is This Important (WITI) test is applied to clustered "Information System Usability Objectives;" and

b. List of Fundamental and Means objective clusters are developed;

Interviews: All the interviews will be conducted either in person or on phone, depending on the availability of the research participants. The goal of these interviews with the research participants is to obtain their values on information system usability. Specially, the interviews will focus on understanding and eliciting the raw usability values of the system users in relation to the information systems usability. Interview is defined as a series of questions presented orally by an interviewer and are usually responded to orally by the research participants (Gliner and Morgan 2000). In this research, we conduct in depth unstructured face-to-face or phone interviews to get detailed responses from the research participants.

Population: The population of research participants is independent information system developers and users who either currently are or have engaged in independent consulting of software development projects. The research participants are working professionals who are over the age of 18 and located in USA. Moreover, research participants have significant experience using IT in their day-to-day jobs and they come from a variety of industries including Federal Government Consulting, financial services industry and

software consulting. For privacy reasons, no personal or demographic information was collected about the research participants.

Survey Instrument: Each research participant will be individually given a brief verbal overview of the VFT and the principles underlying the current research methodology, with specific emphasis on defining values and expressing values surrounding information system usability. Then, the research participants will be presented with a brief definition of the word information system usability. Research participants will be asked to think of any system that they may be using or are familiar with as a reference point and list their values, feelings and wishes with respect of information system usability in their own words. After the research participants listed the usability values in their own words, detailed interviews will be conducted by follow up questions to understand and decipher the meaning of what the research participants have described as information system usability values. See Appendix-A for a copy of the survey instrument that had been used in this research which had received the appropriate Institutional Review Board for approval.

Hierarchies: After eliciting the system developers and users values regarding system usability and converting them into system usability objectives, we leverage the system security objectives developed by Dhillon & Torkzadeh (2006) and use AHP techniques to prioritize the system security and usability objectives and arrange them in hierarchies. For purposes of consistency and simplicity, we had manually performed the analysis involving in AHP techniques. No software program is used for the purpose of AHP.

Case Analysis: After the information system security and usability objective clusters are developed, we also review a case of computer hacking (Perez 2005) and discuss how

several of the security and usability objective clusters identified in this research are either applicable or not applicable for this published case. In this case analysis, we also discuss the conflicting objectives, which contributed to the situation that arose in this case study.

3.5 Conclusions

System developers and users from who have extensive experience in software development and usage have been interviewed to elicit their values within the context of system usability and these values were converted into system usability objectives. Keeney's (1992) VFT methodology was used to determine the system users' values about information system usability and convert the values into system usability objectives. The resultant system usability objectives and the system security objectives developed by Dhillon & Torkzadeh (2006) were prioritized using AHP.

As noted above, VFT and AHP are proven research methodologies within the information system research. Data collection and analysis of data is described in the next four chapters. Chapter four discusses the value-focused thinking analysis and chapter five discusses the AHP analysis. Chapter six analyzes a published case and chapter seven discusses the results and overall implications to information systems research.

Chapter 4 – Usability Objectives Data & Analysis

4.1 Background

In general, information system users prefer ease of use with minimal security controls. However, owners and developers prefer security to minimize any risks relating to legislation, financial, fiduciary and reputation. In recent years, particularly due to Sarbanes-Oxley compliance initiatives, Gramm-Leach-Bliley Act and Health Insurance Portability and Accountability (HIPPA) regulations and other information privacy and security regulations in the United States of America (USA), systems security and privacy of data stored in computer based information systems have become a high priority of many organizations. A PricewaterhouseCoopers LLP (PwC) 15th annual Global Chief Executive Officers (CEO) Survey revealed that 56% of CEOs in the U.S. believe that the "pervasive use of the internet and social media will catapult data privacy and security risks to a higher perch on the risk agenda" (PriceWaterhouseCoopers 2012, p.16). Moreover, several of the regulatory requirements as well as changing organizational needs have brought the information security to the forefront at the expense of the information system usability. This dramatic shift towards prioritization of information system security has given rise to, among the other things, conflicts between systems security requirements and systems usability requirements.

In addition, the information systems research and practice communities have only been able to address the issues of systems security and systems usability in a limited manner by independently focusing either on one or the other. The systems security and usability requirements heavily depend upon the purpose for which the information system is conceived, developed and implemented, the data that is stored and processed in the

information system. Also, the security and usability requirements are dependent on the context in which the computer based information system is used within an organization. Understanding the context in which these systems are used is necessary to incorporate both the security and usability requirements in the computer based information system. Limited research has been conducted to understand the security and usability requirements from the stakeholders' point of view. These stakeholders include system owners, developers, users and security and usability professionals.

Dhillon & Torkzadeh (2006) used the Value Focused Thinking (VFT) approach to identify information system security values in organizations. Application of the VFT approach brought in fresh perspective to the information system security research in that this particular methodology specifically identifies what is valuable to the information system security professionals. However, information system usability has not been understood from the viewpoint of information system developers and users using VFT approach. Applying similar research technique of value focused thinking, we argue that it is imperative to study, understand and identify the values regarding the information system usability from system developers' and users' perspective.

The purpose of this chapter is to present the data collection as well as data analysis of usability objectives from information system developers' and users' perspective. Data was collected from research participants who are independent information system users and developers spread across the USA. Therefore, the information system usability objectives discussed in this paper are not specific to any industry or to any group of industries or to any specific geographical region of USA.

4.2 Research Methods

As discussed by Dhillon & Torkzadeh (2006), data analysis using VFT involves multiple steps and multiple iterations of some of these steps. Using a similar approach followed by Dhillon & Torkzadeh (2006), data collection and analysis for the identification of information system usability objectives from information system users' perspective involves the following distinct processes and sub-processes:

1 Interviews:

- Eliciting "raw usability values" from research participants; and
- Converting "raw usability values" into "cleaned up usability values;"

2 Common Form Usability Values:

- "Cleaned up usability values" are converted into "common form usability values;"
- Duplicate or redundant "common form usability values" are eliminated or merged;
- Unique "common form usability values" are converted into "usability sub-objectives;" and
- Based on similarity, "usability sub-objectives" are clustered and labeled as "usability objectives;"

3 Information System Usability Objectives:

- Why is this important (WITI) test is applied to clustered "Information System Usability Objectives;" and
- List of Fundamental and Means objective clusters are developed;

Though it was suggested by Dhillon & Torkzadeh (2006), due to operational reasons, we have not performed the validation of the system usability values by a panel of experts in this usability values research. However, a published case study has been analyzed to

identify which security and usability objectives indentified from this research are implemented or missing from the published case setting.

4.3 Interviews

Raw values

The goal of the interviews with the research participants is to obtain their values on information system usability. Specially, the interviews were focused on understanding and eliciting the raw usability values of the research participants (system developers and users) in relation to the information systems usability.

The population of research participants consisted of independent information system developers and users who either currently were or had engaged in independent consulting of software development projects. The research participants were male and female working professionals who were over the age of 18 and located in the USA. Moreover, research participants had significant experience using IT in their day-to-day jobs and they come from a variety of industries including Federal Government Consulting, financial services industry and software consulting. Therefore, the information system usability objectives discussed in this chapter are not specific to any one particular industry or to any group of industries or to any specific geographical region of the USA. There were 35 research participants who voluntarily participated in the current study and no personal information about the research participants was collected that would identify and link the research data to specific individual research participants.

Each research participant was individually given a brief verbal overview of the VFT and the principles underlying the current research methodology with specific emphasis on the definition of values and how to think critically to understand and express values

surrounding information system usability. After that, the research participants were presented with a brief definition of the term "information system usability." Then, the research participants were asked to think of any system that they had been using or were familiar with as a reference point and list their values, feelings and wishes with respect of information system usability in their own words. See Appendix-A for the survey instrument that was given to the research participants.

After the research participants listed the usability values in their own words, detailed interviews were conducted with follow up questions to understand and decipher the meaning of what the research participants have described as information system usability values. For example, one research participant indicated "cryptic error messages" as a value. Upon further questioning and follow up explanation, it was derived that the research participant was frustrated with the type of error messages that were given out by the reference information system and the research participant expressed a desire that the error messages were more detailed and less technical. As such, the interviews and follow up questioning helped clarify the context and meaning behind the values, which had been very helpful for further data analysis.

The values collected from the all 35 research participants were considered as "raw usability values". For example, some values described or written by the research participants were in broken or incomplete sentences. See "Raw Values" column in Appendix-B for the entire list of 415 "raw usability values."

Cleaned Up Usability Values

The above collected "raw usability values" are required to be cleaned up for any further analysis. During this process, based on the interviews with the research participants,

significant effort had been made to preserve the nature of the underlying "raw usability values" of the research participants while converting "raw usability values" into "cleaned up usability values." In addition, researcher's judgment was also used wherever necessary during the process of cleaning up and converting "raw usability values" into "cleaned up usability values" to make the system user values readable and useful for further analysis.

For example, one of the "raw usability values" obtained from a research participant read "As far as EMS system is concerned, would want a more user-friendly version, more accurate with schedules, more flexible for users." This "raw usability value" was converted as "cleaned up usability value" to read as "I wish the system is user friendly, with better version control and accuracy and flexibility." As can be seen from this example, in the process of converting "raw usability values" into "cleaned up usability values", every effort had been made to preserve the true nature of the "raw usability value" expressed by the research participants. See "Cleaned-up Raw Values" column in Appendix-B for the entire list of 415 "cleaned up usability values."

4.4 Common Form Usability Values

Common Form Usability Values

Once the "raw usability values" are transformed into "cleaned-up usability values", each "cleaned up usability value" had been converted into a "common form value." The primary goal in the process of "cleaned up usability values" into "common form usability values" was to consolidate similar sounding information system usability values into one "common form value." Another goal in the process of converting "cleaned up values" into "common form values" was to describe the information system usability values.

However, each “cleaned up value” may contain more than one information system usability value. In those cases, one “cleaned up usability value” might generate multiple “common form usability values”.

In addition, the process of converting “cleaned up usability values” into “common form usability values” also partly depends on researcher’s judgment. However, every effort was made to preserve the true nature of the underlying “cleaned up usability values” by keeping in mind one of the primary research question of “how the research participants’ usability values contribute to the information system usability?”

Continuing with example described in the above paragraphs, a “cleaned up usability value” which read as “I wish the system is user friendly, with better version control and accuracy and flexibility” had been converted as a “common form usability value” which read as “I wish the system has better version control.” As noted in this example, the “common form usability value” relate to one and only one information system usability value, which was “version control.” However, the related “cleaned up usability value” also identified two other information system values, namely system flexibility and accuracy as related to process and data. These information system usability values were captured separately in other “common form usability values” namely, “I wish the system allows flexibility in accomplishing tasks”, “Maximize process execution accuracy” and “Maximize accuracy of information generated.”

Unique Common Form Usability Values

After converting all 415 “cleaned up usability values” into “common form usability values”, the first iteration of identifying and removing duplicate “cleaned up usability

values" resulted in 164 "common form usability values." See Appendix-C for the entire list of 164 "common form usability values."

After the first iteration, we re-evaluated all the 164 "common form usability values" for any opportunities to consolidate the "common form usability values." For example, "common form usability value" such as "I wish the system can assign functionality easily and conveniently" can be combined. Upon further review of the 164 "common form usability values", it was noted that there are 37 "common form usability values" that were similar to some other "common form usability values" and can be merged with them. For example, one of the "common form usability values" read as "I wish the system has the ability to post closing transactions" which highlighted the usability value of "system clarity." This specific usability value had already been captured in another existing "common form usability values" which read as "I wish the system has clarity", which also highlights the same usability value of "system clarity." Though the above referenced two "common form usability values" are slightly different in their syntax, they espouse the same usability value. Hence, the former "common form usability value" which espouses the value of "system clarity" has been merged with the latter. As a result of this exercise, 127 unique "common form usability values" had emerged.

Usability Sub-objectives

Based on results of the process described above, the 127 unique "common form usability values" were converted into "usability sub-objectives." Each "usability sub-objective" begins with words such as minimize, maximize, improve, enhance, etc. and highlights the respective usability value that was captured in the "common form usability value." For example, a "common form usability value" which read "I wish the system had clarity"

has been converted into a “usability sub-objective” which read as “Maximize system clarity.” As can be seen from this example, the “usability sub-objective” still underscores the usability value of system clarity. Once again, as noted in above discussed sub-processes, greater attention had been paid to preserve the true nature of the underlying value while converting the “common form usability values” into “usability sub-objectives.” This exercise resulted in 127 “usability sub-objectives.” See Appendix-D for the entire list of 127 “usability sub-objectives.”

Usability Objectives

The primary goal of this sub-process was to take the above generated 127 “usability sub-objectives” and cluster them into several groups that highlight the values of information system usability. This process was needed because each “usability sub-objective” leads to one “usability objective” and each usability objective ultimately enhances the information system usability. This process had been performed by printing out the 127 “usability sub-objectives” on note cards and ordering and clustering them in several iterations until each cluster of “usability objectives” consists of relevant “usability sub-objectives.” After ordering and clustering the “usability sub-objectives” into multiple clusters, each cluster was given a name. Similar to the process of converting “common form usability values” into “usability sub-objectives”, each cluster of “usability sub-objectives” was labeled using words such as minimize, maximize, improve and enhance to highlight the respective usability value that was captured in the “usability sub-objective.” For example, in the following illustration, the bolded sentence was the “usability objective” which encompasses three “usability sub-objectives”, all of which

highlight the value of system access. And maximizing system access ultimately enhances the information system usability.

Maximize system access

Define role-based external access
Ensure authorized external access
Minimize system unauthorized access

The above exercise resulted in 24 clusters and each cluster was labeled to represent one "usability objective." See Appendix-D for the entire list of 127 "usability sub-objectives" and their respective "usability objectives." See table 4.1 for all the 24 "usability objectives" and associated "usability sub-objective" count.

Table 4.1. Information System Usability Objectives and associated Common Form Values' count

Objective No.	Information System Usability Objectives	Associated Common Form Values' count
1	Maximize system maintainability	6
2	Maximize system integrity	2
3	Maximize task efficiency	3
4	Enhance system related communications	6
5	Maximize system administration functionality	4
6	Maximize system reliability	4
7	Clarify & improve system documentation	2
8	Maximize system access	3
9	Maximize system capability	10
10	Maximize standardization of system features	5
11	Maximize productivity	5
12	Maximize system esthetics	8
13	Minimize system interruptions	4
14	Maximize ease of use	9
15	Improve system search capability	3
16	Maximize database and system access	5
17	Maximize system integration	6
18	Maximize self-efficacy in training	7
19	Improve data organization	3

20	Maximize system efficiency	6
21	Maximize disaster recovery	4
22	Maximize data quality	6
23	Maximize security & privacy	8
24	Maximize user requirements elicitation	8
	Total	127

4.5 Information System Usability Objectives

Why Is This Important (WITI) test

The primary goal of this sub-processes of data analysis it to answer the question of "Why is this important (WITI)?" by taking information system usability objectives identified in the above process and classifying them into "fundamental" and "means" objectives. Such a classification would help understand the developers' and users' perspectives of information system usability at a deeper level. Keeney (1992) noted that classification of objectives as "fundamental" and "means" categories is a subjective and interpretive process (p. 157). However, he argues that such a classification of objectives is the ultimate tool that would help in maximizing the usability of a computer based information system. Means objectives are merely a way to achieve the fundamental objectives (Keeney 1992). Classification of usability objectives into means and fundamentals is critical to making informed decisions about usability of an information system. The application of the WITI test to all the usability objectives identified in this study resulted in eight fundamental and 16 means objectives. In this research context of system usability requirements from system developers' and users' perspectives, the fundamental objectives lead to the overall system usability and the means objectives lead to one or more of either the fundamental objectives or means objectives.

Fundamental Objective & Means Objective Clusters

Fundamental Objective Clusters: Based on the WITI test, this study identified the following eight fundamental objective clusters that would help maximize usability in an information system.

Maximize system integrity: System integrity could be maximized by maximizing the system adaptability to changing user requirements and by maximizing the system reliability in performing the system functionality. Increased system integrity leads to increased system usability.

According to US-CERT's Technical Information Paper-TIP-11-075-0 dated March 16, 2011, two key components of system integrity are software authenticity and assurance of user identity (US-CERT 2011). Ensuring the use of authentic software only by those authorized would maximize the system integrity.

Maximize data quality: Strong and Volkoff (2010) note that data quality issues such as inaccuracy, inconsistent data representations, inaccessibility to data, lack of timeliness data or inappropriate of data might cause data misfit in an Enterprise System. Hence, maximizing the data quality, also improves the system usability to help avoid any data misfits between computer based information system and the system users.

System data quality could be maximized by giving appropriate user warnings prior to data deletion, by ensuring accuracy in data processing, transmission and storage and enabling data interoperability. Increased data quality leads to increased system usability.

Maximize productivity: DiAngelo and Petrun (1995), while studying the product based usability requirements, discuss that if customers (users) spend their time in performing activities that deal with the tool (system) such as (for example, in the case of a word processing tool) adjusting the margins, fonts and format, this will result in decreased

productivity and customer (user) satisfaction. From software development point of view, system usability includes attributes of a system that affect productivity (Seffah and Metzker 2004). In addition, Schultz, Proctor et al. (2001), in their study of a new authentication mechanism for an information system, highlighted the issues such as complicated user interaction tasks and timing complications that had at first lowered user productivity considerably.

System users' productivity could be maximized by automating user administration activities, by minimizing system users' interaction with the help desk and by appropriate system functionality. Increased productivity leads to increased system usability.

Maximize ease of use: As early as in 1995, it has been established that ease of use is one of the critical factors required for the usability of a product (information system) (DiAngelo and Petrun 1995). DiAngelo and Petrun (1995) study identified that some of the ease of use characteristics include information presentation, use of graphics and time it takes to do a task. Saltzer and Schroeder (1975) defined the principle of psychological acceptability which highlights that security features in the information system must be designed for ease of use so that users routinely and automatically apply these protection mechanisms correctly.

System ease of use could be maximized by enhancing system navigation features, by simple, yet visually appealing and user friendly, presentation of features and functionality and by incorporating intuitive or easy to learn features and functionality. Enhanced ease of system use leads to increased system usability.

Maximize security and privacy: Zurko and Simon (1997) proposed the concept of user centered security which allows usability as the primary goal for security. Gunson,

Marshall et al. (2011), in their study of user perceptions of security and usability of single-factor and two-factor authentication in automated telephone banking, discovered that typically users prefer the lower security mechanisms as a trade off for the usability. System security and privacy could be maximized by collecting, protecting, storing and handling personal data in a secure manner and by compartmentalizing access to the system on a need to know basis. Increased security and privacy leads to increased system usability.

Maximize system capability: When an information system does not meet the user requirements due to usability issues, users tend to create workarounds to accomplish the missing systems capabilities (Johnson and Willey 2011).

System capability could be maximized by making system capable of processing various types of transactions and data (such as different currencies), by providing multiple platform (Windows, Unix, etc.) and language availability and support and by delivering useful metrics and reporting features. Increased system capability leads to increased system usability.

Maximize system integration: System integration in information systems, especially in emergency systems, is necessary for maintenance of smooth business operations (Paulheim, Doweling et al. 2009). In the 2009 draft Study Group Report on System Integration by Canadian Software and Systems Engineering Secretariat, it was noted that enterprise integration efforts fail due to, among several other reasons, a number of technical reasons including changing needs for interoperability, performance, security, and usability (JTC1/SC7 2010).

System integration could be maximized by organizing various system features in an intuitive way and organized way, by making the system easy to navigate and operate and by enhancing the visual appearance. Increased system integration leads to increased system usability.

Maximize system reliability: In a study of manufacturer incentives to invest in the improvement of reliability and security of a software system, it was confirmed that software bugs cause the system reliability and system security failures (Honeyman, Schwartz et al. 2007).

System reliability could be maximized by maximizing process execution accuracy, by providing reliable real-time processing capabilities and by minimizing the application related risks. Increased system reliability leads to increased system usability.

Means Objective Clusters: The above eight fundamental objectives could be achieved with all or any of the following 16 means objectives which indirectly contribute to the overall system usability:

Enhance system related communications: Debrabander and Edstrom (1997) argued that the central problem in the communications between system developers and system users is that both parties bring different conceptual frameworks to their interactions in the system development process. Debrabander and Edstrom (1997) consider the interaction process between a potential user and a system developer as a dyadic relationship and suggest effective communication patterns while preserving the nature of different perspectives that these two parties bring to the interaction process.

System related communications could be enhanced in several ways including by making the information system more responsive, by increasing the transaction processing speed,

by communicating system changes in a better way and by instituting an efficient two-way feedback. Such an enhancement in system related communications could maximize other means objectives of system usability such as maximize system maintainability, maximize system disaster recovery time and improve overall data organization, which ultimately contribute to the fundamental objectives of system usability.

Maximize system efficiency: Lack of sufficient power, software bugs and issues related to the user interface design, among several other issues reduce the system efficiency (Karlsson 2000).

System efficiency could be maximized by ensuring process fairness and by enhancing system functionality based on user feedback. Such an enhancement in system efficiency could maximize other means objectives of system usability such as maximize system maintainability, maximize system disaster recovery time and improve overall data organization, which ultimately contribute to the fundamental objectives of system usability.

Maximize system maintainability: Folmer, Gurp et al. (2003) note that software system quality attributes such as system performance and system maintainability are determined by the overall system architecture and require special attention during the system development process in order to achieve the required levels of system performance and maintainability.

System maintainability could be maximized by automating the system upgrades, by minimizing the system configuration changes, by setting up minimum standards for system configuration and by minimizing system total cost of ownership. Maximizing system maintainability would ultimately contribute to the fundamental objectives of system usability.

Maximize disaster recovery: System disaster recovery could be maximized by ensuring that system is available without any interruptions and by instituting a process to regularly back up critical system configurations and data and by regularly testing the disaster recovery procedures. Maximizing system disaster procedures would ultimately contribute to the fundamental objectives of system usability.

Improve data organization: Data organization could be improved in several ways including by enabling data archival and retrieval features in a user friendly and visually appealing manner. Improving data organization would ultimately contribute to the fundamental objectives of system usability.

Maximize self-efficacy in training: Self-efficacy in training could be maximized by providing appropriate training to the system users, by providing on-line help and manuals that are context specific and by providing easily accessible user support. Maximization of self-efficacy in system training would ultimately contribute to the fundamental objectives of system usability.

Clarify & improve system documentation: System documentation could be clarified and improved with well written procedures and easy accessibility. Clarification and improvement of system documentation would ultimately contribute to the fundamental objectives of system usability.

Maximize task efficiency: Strong and Volkoff (2010) argue that usability misfits occur when user interactions with the system are cumbersome or confusing (p.737).
System task efficiency could be maximized by providing flexibility to system users in performing system related tasks. Maximization of task efficiency would ultimately contribute to the fundamental objectives of system usability.

Maximize system administration functionality: System administration functionality could be maximized by allowing users to manage various functions and features without too much interaction from the system administrators and by automating various administrative account features and functions. Maximization of system administration functionality would ultimately contribute to the fundamental objectives of system usability.

Maximize standardization of system features: Standardization of system features could be accomplished in several ways including by minimizing individual system customization and maximizing standardization across multiple functionalities. Maximization of system standards could maximize productivity and ease of system use, which ultimately improves the system usability.

Maximize system esthetics: System esthetics could be maximized by presenting the process and functionality of the system in a visually appealing way. Maximization of system esthetics could maximize productivity and ease of system use, which ultimately improves the system usability.

Improve system search capability: Improving system search capability for system-help topics and presenting the results in a visually appealing and user friendly way could maximize productivity and ease of system use, which ultimately improves the system usability.

Minimize system interruptions: System interruptions could be minimized in several ways including by ensuring freeze-free processing and unnecessary lock-outs and by minimizing any system outage and delays. Minimizing system interruption could

maximize productivity and ease of system use, which ultimately improves the system usability.

Maximize system access: System access could be maximized by linking access levels to the organizational roles and by minimizing unauthorized access through the use of various tools. Maximization of system access could ultimately contribute to the fundamental objectives of system usability.

Maximize database and system access: System and database access could be maximized by periodic turning and optimizing the functions of the application database access and by supporting the critical applications with real-time databases. Maximization of database and system access could ultimately contribute to the fundamental objectives of system usability.

Maximize user requirements elicitation: System user requirements elicitation process could be maximized by building-in automated internal controls, by incorporating collaborative features into the system, by turning and optimizing the function of the application database access and by supporting the critical applications with real-time databases. Maximization of database and system access could ultimately contribute to the fundamental objectives of system usability.

4.6 Conclusion

We interviewed 35 research participants and obtained the values that they consider critical for information system usability. These usability values were analyzed and organized in to eight "fundamental objective clusters" and 16 "means objective clusters." In the following chapter, the above identified usability objective clusters are compared with the security objectives proposed by Dhillon and Torkzadeh (2006) to identify any common objectives to help align security and usability objectives for computer based information systems.

Chapter 5 – Security and Usability Objectives: Comparative Analysis using AHP

5.1 Introduction

As noted in Chapter 3, methodologically, this research is based on Keeney's (1996) "value focused thinking' (VFT) approach. Firstly, the goal of this research was to identify the information system usability objectives. This research was performed and described in detail in chapter 4 above. Secondly, by using information system usability objectives developed from this research as well as the information system security objectives developed by Dhillon and Torkzadeh (2006), it is also the goal of this research to perform a comparative analysis of the information system security and usability objectives. The purpose of this comparative analysis was to identify any security and usability objectives that are similar or conflicting with each other and to arrange security and usability objectives in an organized manner.

We define a comparative analysis for the purposes of this research as objectively prioritizing the security and usability objectives using the principles and concepts of Analytic Hierarchy Process (AHP) methodology. The result of this comparative analysis was potential hierarchies of information system security and information system usability objectives. Since both the information system security and usability objectives were obtained using VFT approach, we believe that a detailed comparative analysis of security and usability objectives was appropriate as these two sets of objectives were derived using the same methodology. As such, in this chapter, we demonstrate how the security and usability fundamental and means objectives can be tailored to create security and usability hierarchies that are specific to a particular business or operational context.

5.2 Information System Security Objectives

Dhillon and Torkzadeh (2006) conducted a value-focused assessment of information system security in organizations and proposed nine "fundamental objective clusters" and 16 "means objective clusters." As noted by the authors as well as Keeney (1996), the "means objectives" either directly or indirectly contribute to help achieve one or more of the fundamental objectives. The nine "fundamental objective clusters" are described below in table 5.1 along with an example of objectives that is part of each underlying "fundamental objective cluster." For easier reference in the following paragraphs, each of the objectives noted in the table 5.1 was given a unique identifier, namely, Security Fundamental Objective-1 (SFO-1), SFO-2, etc.:

Table 5.1. Information System Security - Fundamental objectives

Fundamental Objective (9 clusters)	
Enhance management development practices (SFO-1) e.g.: Provide employees with adequate IT training	**Provide adequate human resource management practices (SFO-2)** e.g.: Enhance individual/group pride in the organization
Develop and sustain an ethical environment (SFO-3) e.g.: Create an environment that promotes organizational loyalty	**Maximize access control (SFO-4)** e.g.: Ensure physical security
Promote individual work ethic (SFO-5) e.g.: Minimize temptation to use information for personal benefit	**Maximize data integrity (SFO-6)** e.g.: Minimize unauthorized changes
Enhance integrity of business processes (SFO-7) e.g.: Ensure that appropriate organizational controls (formal and informal) are in place	**Maximize privacy (SFO-8)** e.g.: Emphasize importance of rules against disclosure
Maximize organizational integrity (SFO-9) e.g.: Create an environment of managerial support and solidarity	

The 16 "means objective clusters" are described below in table 5.2 along with an example of objectives that is part of each underlying "means objective cluster." For easier reference in the following paragraphs, each of the objective noted in the table 5.2

was given a unique identifier, namely, Security Means Objective-1 (SMO-1), SMO-2, etc.:

Table 5.2. Information System Security - Means objectives

Means Objectives (16 clusters)	
Increase Trust (SMO-1) e.g.: Develop an environment that promotes a sense of organizational responsibility	**Provide open communication (SMO-2)** e.g.: Create an open-door environment within all levels of the organization
Maximize awareness (SMO-3) e.g.: Ensure explicit understanding of organizational culture by individuals	**Optimize work allocation practices (SMO-4)** e.g.: Develop understanding of organizational and information use procedures
Establish ownership of information (SMO-5) e.g.: Promote ownership in the organization	**Clarify centralization/decentralization issues (SMO-6)** e.g.: Ensure a right balance between centralization and decentralization
Ensure legal an procedural compliance (SMO-7) e.g.: Decrease the level of employer's tolerance for misuse of information	**Improve authority structures (SMO-8)** e.g.: Clarify delegation of authority
Ensure availability of information (SMO-9) e.g.: Ensure adequate procedures for availability of information	**Promote responsibility and accountability (SMO-10)** e.g.: Clarify delegation of responsibilities
Understand work situation (SMO-11) e.g.: Minimize creation of disgruntled employees	**Maximize fulfillment of personal needs (SMO-12)** e.g.: Appreciate personal needs for job enhancement
Understand individual characteristics (SMO-13) e.g.: Interpret individual lifestyles	**Enhance understanding of personal financial situation (SMO-14)** e.g.: Eliminate personal benefit of sharing information with competitors
Ensure censure (SMO-15) e.g.: Instill a fear of consequences	**Understand personal beliefs (SMO16)** e.g.: Minimize the need for greed in the organization

5.3 Information System Usability Objectives

As noted in chapter 4 – data analysis, using VFT approach, we had identified the information system usability objectives. The objectives were then arranged in clusters to unearth the real meanings and the values associated with each of these objectives. This categorization resulted in eight "fundamental objective clusters" and 16 "means objective clusters."

The eight "fundamental objective clusters" are described below in table 5.3 along with an example of objectives that is part of each underlying "fundamental objective cluster." For easier reference in the following paragraphs, each of the objective noted in the table 5.3 was given a unique identifier, namely, Usability Fundamental Objective-1 (UFO-1), UFO-2, etc.:

Table 5.3. Information System Usability – Fundamental objectives

Fundamental Objective (8 clusters)	
Enhance system related communications (UFO-1) e.g.: Ensure exception reports go to management	**Maximize system administration functionality (UFO-2)** e.g.: Enhance connectivity at affordable price
Improve data organization (UFO-3) e.g.: Ensure data archival functionality	**Maximize system capability (UFO-4)** e.g.: Enhance application features
Maximize ease of use (UFO-5) e.g.: Ensure ease of navigation through application	**Maximize system integration (UFO-6)** e.g.: Ensure functionality is designed into system
Maximize standardization of system features (UFO-7) e.g.: Enhance customizable interfaces	**Maximize user requirements elicitation (UFO-8)** e.g.: Ensure system functionality meets requirements

The 16 "means objective clusters" are described below in table 5.4 along with an example of objectives that is part of each underlying "means objective cluster." For easier reference in the following paragraphs, each of the objective noted in the table 5.1 was given a unique identifier, namely, Usability Means Objective-1 (UMO-1), UMO-2, etc.:

Table 5.4. Information System Usability - Means objectives

Means Objectives (16 clusters)	
Clarify & improve system documentation (UMO-1) e.g.: Ensure easy access to system documentation	**Maximize system access (UMO-2)** e.g.: Define role-based external access
Improve system search capability (UMO-3) e.g.: Ensure semantic based search features	**Maximize system efficiency (UMO-4)** e.g.: Ensure process fairness
Maximize data quality (UMO-5) e.g.: Enhance data integrity	**Maximize system esthetics (UMO-6)** e.g.: Enhance visualization of system security
Maximize database and system access (UMO-7) e.g.: Ensure web access to the system	**Maximize system integrity (UMO-8)** e.g.: Maximize system adaptability
Maximize disaster recovery (UMO-9) e.g.: Ensure data availability	**Maximize system maintainability (UMO-10)** e.g.: Ensure hardware robustness
Maximize productivity (UMO-11) e.g.: Ensure automated password retrieval	**Maximize system reliability (UMO-12)** e.g.: Maximize process execution accuracy
Maximize security & privacy (UMO-13) e.g.: Decrease restrictiveness of system	**Maximize task efficiency (UMO-14)** e.g.: Maximize automation of manual tasks
Maximize self-efficacy in training (UMO-15) e.g.: Enhance system training quality	**Minimize system interruptions (UMO-16)** e.g.: Minimize system down-time

5.4 Comparative Analysis using AHP

As noted in the chapter 3 – literature review, the classical definition of information security consists of three critical security goals, namely confidentiality, integrity and availability. Whereas usability has been defined in several which ways that espouses several usability goals such as ease of use, users' perceptions about ease of use and usefulness, etc., we take the approach adopted by Dzida (1996) where the word usability is defined in terms of "effective, efficient and satisfying performance of the users' task (p. 173)." This information system usability definition highlights three critical usability goals that are relevant for this study, namely effectiveness, efficiency and satisfaction. We believe that this usability definition is relevant for this research since definition considers the usability goals both from product as well as user point of view.

As pointed out by Saaty (1990), in the analytic hierarchy process, all the relevant decision making factors can be arranged in a hierarchical structure descending from an overall

goal to criteria, sub-criteria and alternatives in successive levels. Saaty (1990) also points out that a hierarchy, developed using AHP principles and concepts, is not a traditional decision tree and it does not need to be complete with all levels in the hierarchy. For purposes of the comparative analysis of information system security and usability objectives, we use overall/over-arching goals, "fundamental objective clusters" and "means objective clusters" as analogous to overall goals, criteria and sub-criteria that is necessary to form a hierarchical structure. While the overall/over-arching goals could be any security and usability related goals, we argue that the "fundamental objective clusters" and "means objective clusters" of security and usability identified could form the basis for the typical criteria and sub-criteria respectively because similar complementing nature of the criteria and sub-criteria exists between "fundamental objective clusters" and "means objective clusters." The exercise of developing information system security and/or usability hierarchies involves the following three steps:

- Select one or more of the information system security or usability overall/over-arching goals security goals (of confidentiality, integrity, availability, efficiency, effectiveness and satisfaction).
- Then, identify the "fundamental objective clusters" of information system security and/or usability that are relevant for the overall/over-arching security goals and place them under the information system usability overall/over-arching goals.
- After that, identify the "means objective clusters" of information system security and/or usability that are relevant for the "fundamental objective clusters" and

associate respective “means objective clusters” to the relevant “fundamental objective clusters.”

As such, with the use of AHP concepts for comparative analysis, each resultant hierarchy must have an overall/over-arching goal. For purposes of comparative analysis of the information system security objectives using AHP, we further argue that the overall/over-arching goal of an information system could be any combination of the three critical security goals, namely confidentiality, integrity and availability. To further elaborate this idea, we argue that depending on the context of the information system that is being developed, a computer based information system, along with other non-security related objectives, could have a security objective of keeping the data in the system confidential or protecting the integrity of the data or ensuring the availability of the system or any combination of the above three objectives. For example, for information security purposes, a military or defense oriented information system could have confidentiality as the most important goal. Whereas, a payroll system used within a multi-national corporation could have availability and integrity as the most important goals for information security purposes. The relative selection of the security goals that are suitable for an information system is heavily dependent on the nature and context in which the system is used by the users.

As such, depending on the nature and context within which information systems are used, the security goals, along with other non-security related objectives, of these information systems could be any one of the following overall/over-arching goals:

- A computer based information system with a goal to protect the **confidentiality** of the data.

- A computer based information system with a goal to guard the **integrity** of the data.
- A computer based information system with a goal to ensure the **availability** of the system to authorized users.
- A computer based information system with a goal to protect the **confidentiality** and **integrity** of the data.
- A computer based information system with a goal to protect the **confidentiality** and ensures the **availability** of the data.
- A computer based information system with a goal to guard the **integrity** and ensure the **availability** of the data.
- A computer based information system with a goal to ensure the **confidentiality**, **integrity** and **availability** of the data.

Similarly, for purposes of comparative analysis of the information system usability objectives using AHP, we argue that the overall/over-arching goal of an information system could be any combination of the three critical usability goals, namely efficiency, effectiveness and satisfaction. To further elaborate this idea, we argue that depending on the context of the information system that is being developed, a computer based information system, along with other non-usability related objectives, could have a usability objective of making the system efficient or making the system effective or ensuring that users are satisfied. For example, for information usability purposes, a military or defense oriented information system could have the effectiveness and efficiency as the most important goals. Whereas, a free web-based email system provided to users by an email service provider could have user satisfaction as the most important goals for usability purposes. Similar to security objectives, the relative

selection of the usability goals that are suitable for an information system is heavily dependent on the nature and context in which the system is used by the users.

As such, depending on the nature and context within which information system are used, the information system usability goals, along with other non-usability related objectives, of these systems could be any of the following goals:

- A computer based information system with a goal to be **efficient**.
- A computer based information system with a goal to be **effective**.
- A computer based information system with a goal to ensure the user **satisfaction**.
- A computer based information system with a goal to **efficient** and **effective**.
- A computer based information system with a goal to be **efficient** while ensuring user **satisfaction**.
- A computer based information system with a goal to be **effective** while ensuring user **satisfaction**.
- A computer based information system with a goal to **efficient** and **effective** while ensuring user **satisfaction**.

No computer based information system can focus either only on the information system security goals or only on the information system usability goals. As such, an appropriate balance has to be maintained between the system security and usability goals within the context in which these information systems are implemented and used. In such scenarios, an information system could have any combination of the system security goals (of confidentiality, integrity and availability) and system usability goals (of efficiency, effectiveness and satisfaction). The following are some examples of such goals and please note that this listing of combined information security and usability goals is for

illustration purposes only and was not an exhaustive list of all possible combinations of information security and usability goals:

- A computer based information system with a goal to protect the **confidentiality** of the data while ensuring user **satisfaction**.
- A computer based information system with a goal to ensure the **availability** of the data and user **satisfaction**.
- A computer based information system with a goal to be **efficient** along with a goal to ensure the **availability** of the data and user **satisfaction**.
- A computer based information system with a goal to protect the **confidentiality**, **integrity** and **availability** of the data along with a goal to be **efficient**, **effective** and ensure user **satisfaction**.

5.5 Proposed Hierarchies using AHP

Information System Security Hierarchies

The purpose of this sub-section is to develop hierarchies with an overall/over-arching goal of information system security. As noted in the above sections, the information system security hierarchies could be formed using the overall/over-arching security goals (of confidentiality, integrity and availability), nine "fundamental objective clusters" and 16 "means objective clusters." The exercise of developing information system security hierarchies involves the following three steps:

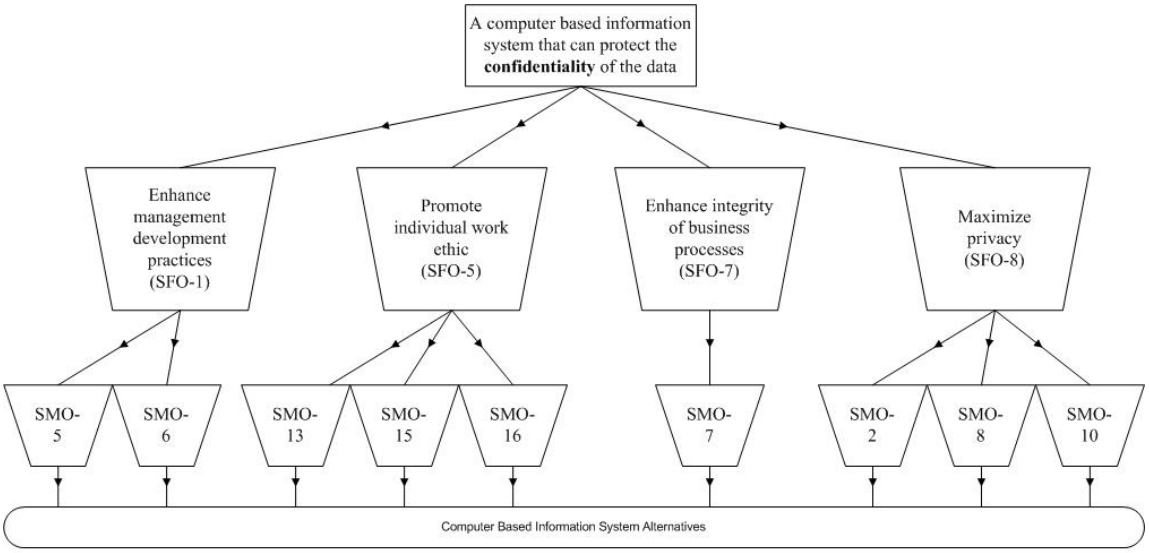
- Select one of the information system security overall/over-arching goals (of confidentiality, integrity and availability).
- Identify the relevant "fundamental objective clusters" of information system security for the above selected overall/over-arching security goal and place all the

"fundamental objective clusters" under the information system security overall/over-arching goal.

- Identify the relevant "means objective clusters" of information system security for the above identified "fundamental objective clusters" and associate the respective "means objective clusters" to the relevant "fundamental objective clusters."

See figures 5.1, 5.2 and 5.3 below for the information system security hierarchies with confidentiality, integrity and availability as overall/over-arching goals respectively:

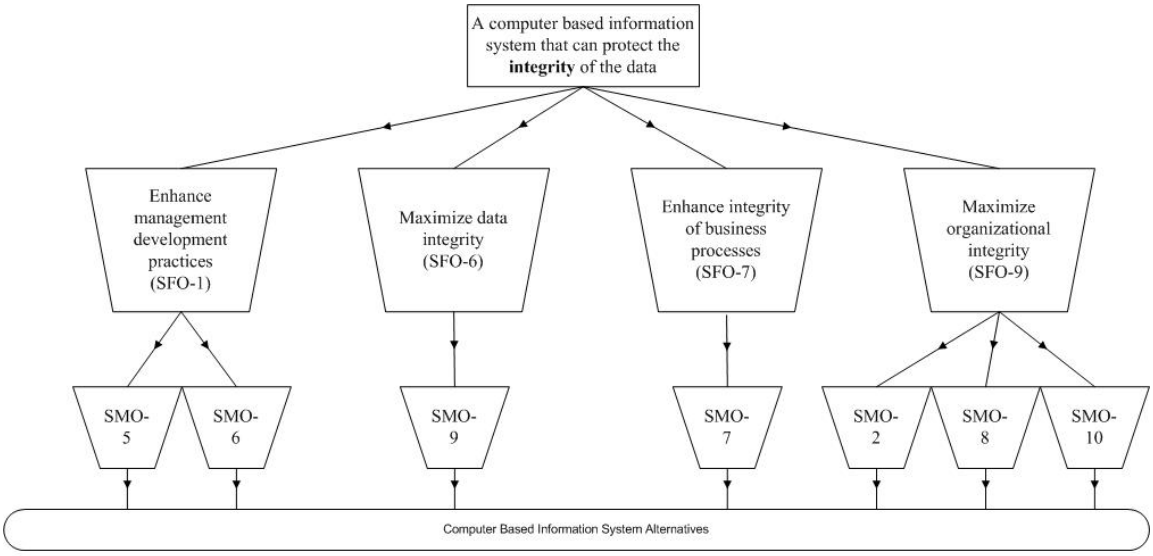
Figure 5.1. Information System Security Hierarchy with **confidentiality** as the overall/over-arching goal



As depicted in the above diagram 5.1, the information system security hierarchy with the overall/over-arching information security goal of protecting the confidentiality of the data can be achieved by focusing on the information security fundamental objectives of

enhancing the management development practices, promoting the individual work ethic, enhancing the integrity of the business processes and maximizing privacy. In addition, this hierarchy also highlights that the relevant security fundamental objectives can be accomplished by meeting the associated security means objectives namely SMO-2, SMO-5, SMO-6, SMO-7, SMO-8, SMO-10, SMO-13, SMO-15 and SMO-16 as identified in the diagram 5.1.

Figure 5.2. Information System Security Hierarchy with integrity as the overall/over-arching goal

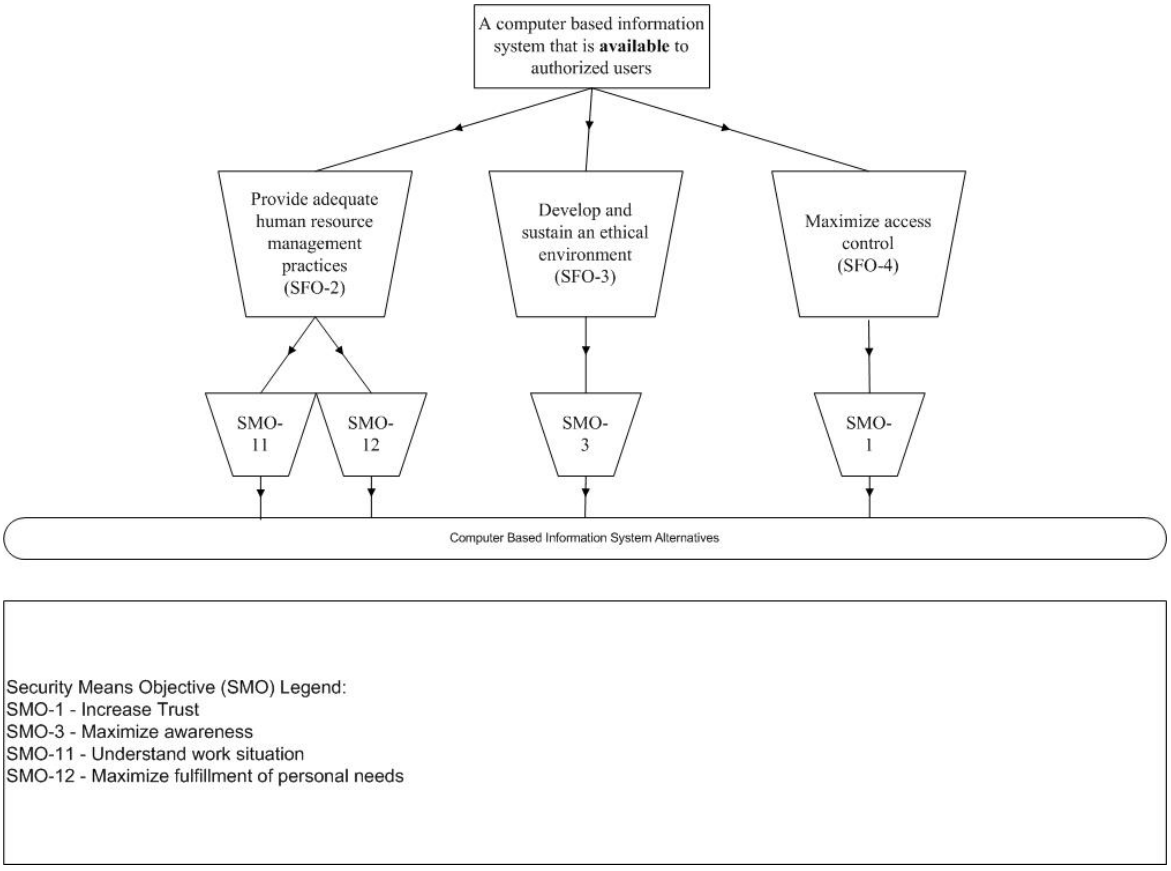


Security Means Objective (SMO) Legend:
SMO-2 - Provide open communication
SMO-5 - Establish ownership of information
SMO-6 - Clarify centralization/decentralization issues
SMO-7 - Ensure legal an procedural compliance
SMO-8 - Improve authority structures
SMO-9 - Ensure availability of information
SMO-10 - Promote responsibility and accountability

As depicted in the above diagram 5.2, the information system security hierarchy with the overall/over-arching information security goal of protecting the integrity of the data can be achieved by focusing on the information security fundamental objectives of enhancing the management development practices, enhancing the integrity of the business processes and maximizing the organizational as well as data integrity. In addition, this hierarchy

also highlights that the relevant security fundamental objectives can be accomplished by meeting the associated security means objectives namely SMO-2, SMO-5, SMO-6, SMO-7, SMO-8, SMO-9 and SMO-10 as identified in the diagram 5.2.

Figure 5.3. Information System Security Hierarchy with **availability** as the overall/over-arching goal



As depicted in the above diagram 5.3, the information system security hierarchy with the overall/over-arching information security goal of ensuring that the availability of the data can be achieved by focusing on the information security fundamental objectives of providing adequate human resource management practices, developing a sustainable ethical environment and maximizing access control protocols. In addition, this hierarchy also highlights that the relevant security fundamental objectives can be accomplished by

meeting the associated security means objectives namely SMO-1, SMO-3, SMO-11 and SMO-12 as identified in the diagram 5.3

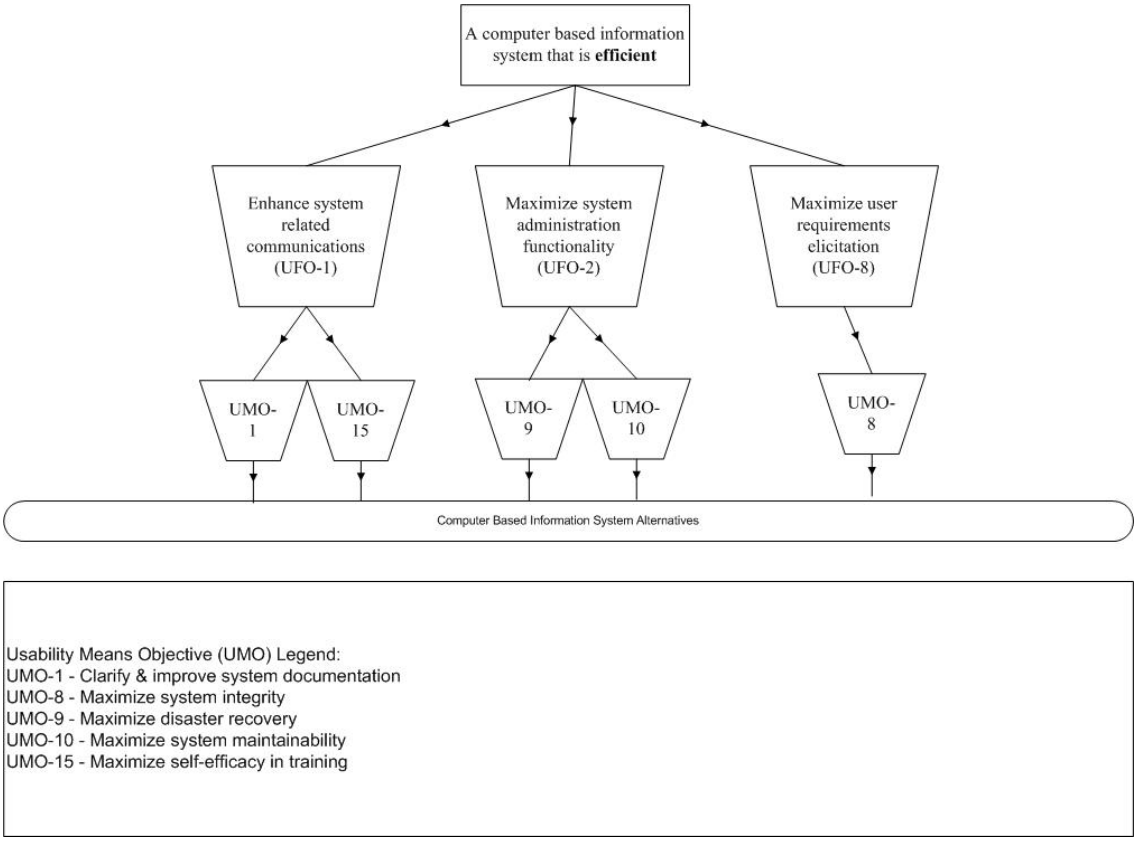
Information System Usability Hierarchies

The purpose of this sub-section is to develop hierarchies with an overall/over-arching goal of information system usability. As noted in the above sections, the information system usability hierarchies could be formed using the overall/over-arching usability goals (of efficiency, effectiveness and satisfaction), eight "fundamental objective clusters" and 16 "means objective clusters." Similar to the information system security hierarchies, the exercise of developing information system usability hierarchies involves the following three steps:

- Select one of the information system usability overall/over-arching goals (of efficiency, effectiveness and satisfaction).
- Identify the relevant "fundamental objective clusters" of information system usability for the above selected overall/over-arching usability goal and place all the "fundamental objective clusters" under the information system usability overall/over-arching goal.
- Identify the relevant "means objective clusters" of information system usability for the above identified "fundamental objective clusters" and associate the respective "means objective clusters" to the relevant "fundamental objective clusters."

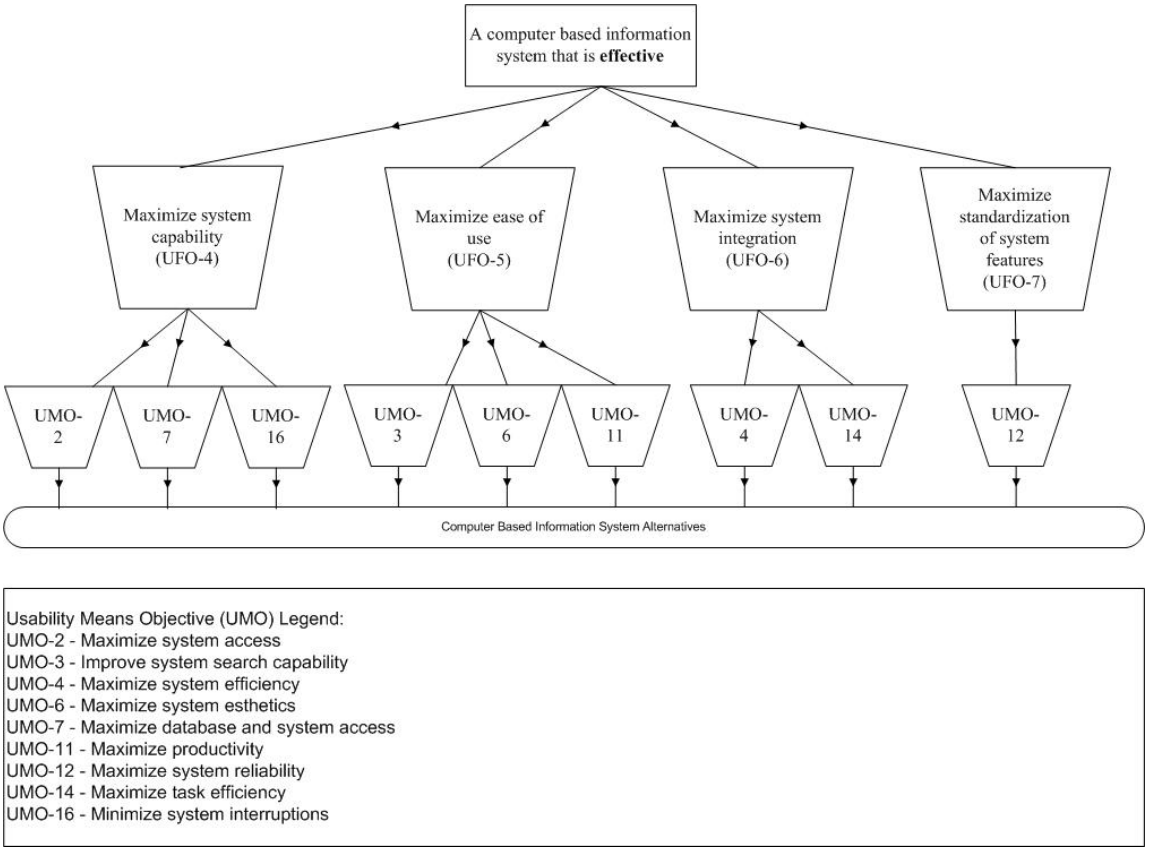
See figures 5.4, 5.5 and 5.6 below for the information system usability hierarchies with efficiency, effectiveness and user satisfaction as the overall/over-arching goals respectively:

Figure 5.4. Information System Usability Hierarchy with **efficiency** as the overall/over-arching goal



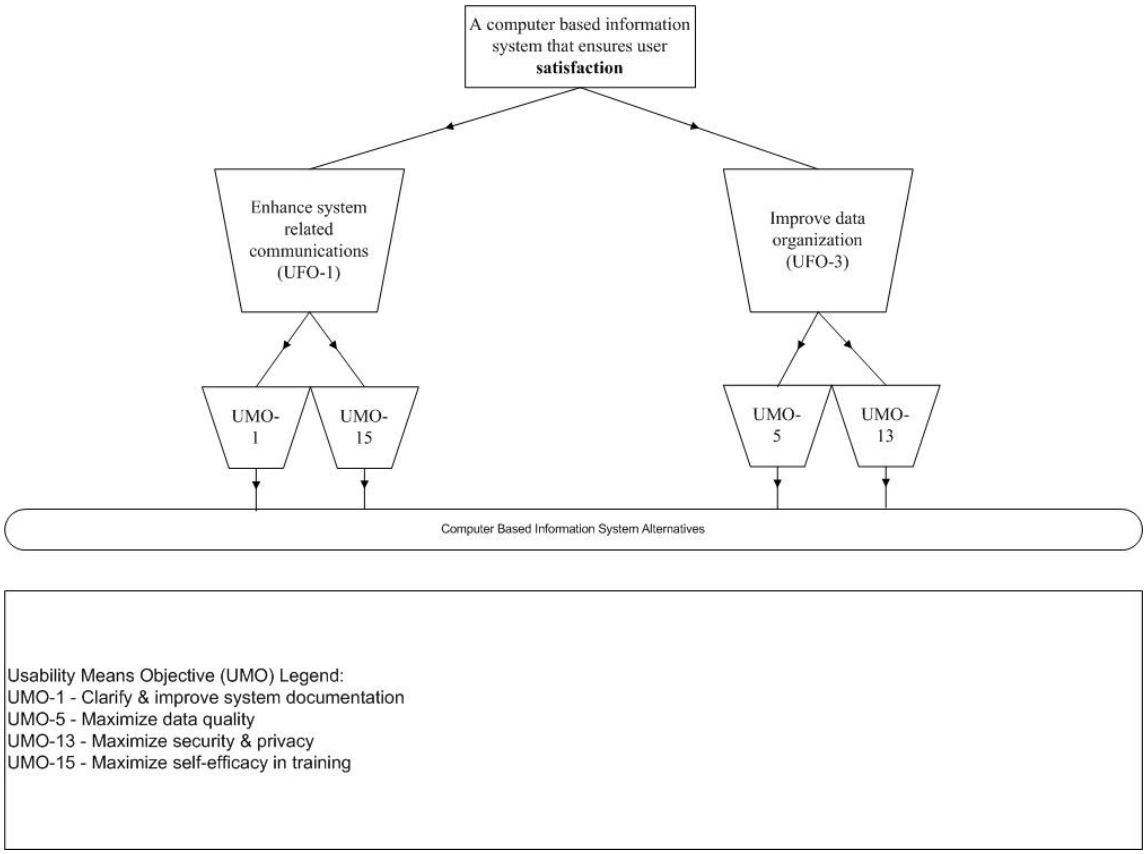
As depicted in the above diagram 5.4., the information system usability hierarchy with the overall/over-arching information usability goal of an efficient system can be achieved by focusing on the information usability fundamental objectives of enhancing system related communications, maximizing system administration functionality and maximizing user requirements elicitation process. In addition, this hierarchy also highlights that the relevant usability fundamental objectives can be accomplished by meeting the associated usability means objectives namely UMO-1, UMO-8, UMO-9, UMO-10 and UMO-15 as identified in the diagram 5.4.

Figure 5.5. Information System Usability Hierarchy with **effectiveness** as the overall/over-arching goal



As depicted in the above diagram 5.5., the information system usability hierarchy with the overall/over-arching information usability goal of an effective system can be achieved by focusing on the information usability fundamental objectives of maximizing system capability, maximizing ease of use, maximizing system integration and maximizing the standardization of system features. In addition, this hierarchy also highlights that the relevant usability fundamental objectives can be accomplished by meeting the associated usability means objectives namely UMO-2, UMO-3, UMO-4, UMO-6, UMO-7, UMO-11, UMO-12, UMO-14 and UMO-16 as identified in the diagram 5.5.

Figure 5.6. Information System Usability Hierarchy with **user satisfaction** as the overall/over-arching goal



As depicted in the above diagram 5.6., the information system usability hierarchy with the overall/over-arching information usability goal of user satisfaction can be achieved by focusing on the information usability fundamental objectives of enhancing system related communications and improving the data organization. In addition, this hierarchy also highlights that the relevant usability fundamental objectives can be accomplished by meeting the associated usability means objectives namely UMO-1, UMO-5 UMO-13 and UMO-15 as identified in the diagram 5.6.

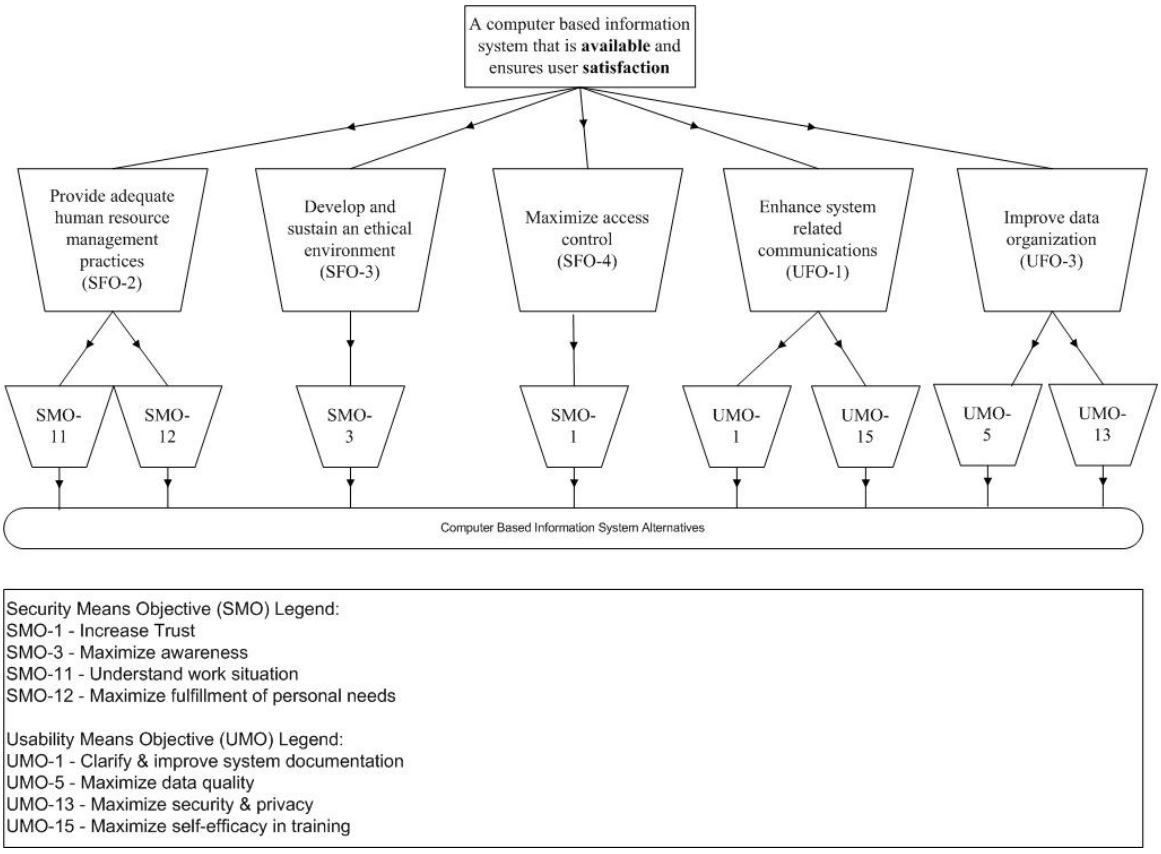
Information System Security and Usability Hierarchies

The purpose of this sub-section is to develop hierarchies with an overall/over-arching goal to include relevant information security and information usability goals (of confidentiality, integrity, availability, efficiency, effectiveness and satisfaction). In accordance with the above security and usability hierarchies, this exercise of developing information system security and usability hierarchies involves the following three steps:

- Select one or more of the information system security overall/over-arching goals (of confidentiality, integrity and availability) and one or more of the information system usability overall/over-arching goals (of efficiency, effectiveness and satisfaction).
- Identify the relevant "fundamental objective clusters" of information system security and usability for the overall/over-arching security and usability goals and place all the "fundamental objective clusters" under the information system security and usability overall/over-arching goals.
- Identify the relevant "means objective clusters" of information system security and usability for the above identified "fundamental objective clusters" and associate the respective "means objective clusters" to the relevant "fundamental objective clusters."

If a computer based information system were to be designed and built with appropriate security and usability goals that are specific to a business or operational context, such a system would to achieve the relevant information system security and usability objectives as discussed in the sections 5.3 and 5.4 above. For example, see figure 5.7 below for the computer based information system security and usability hierarchy with an information system security overall/overarching goal to ensure the availability and an information system usability overall/overarching goal of user satisfaction:

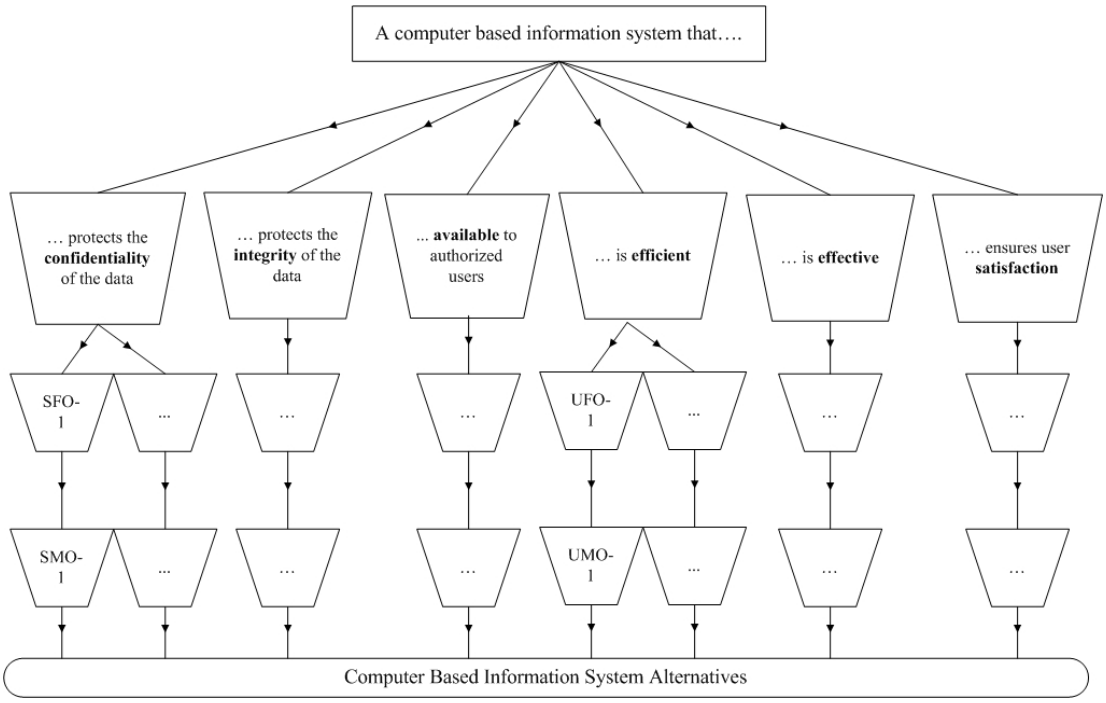
Figure 5.7. Information System Security and Usability Hierarchy with **availability** and user **satisfaction** as the overall/over-arching goals



As depicted in the above diagram 5.7., the combined information system security and usability hierarchy with the overall/over-arching information security and usability goals of availability and user satisfaction can be achieved by focusing on the information security and usability fundamental objectives of providing adequate human resource management practices, developing a sustainable ethical environment, maximizing access control protocols, enhancing system related communications and improving the data organization. In addition, this hierarchy also highlights that the relevant security and usability fundamental objectives can be accomplished by meeting the associated security and usability means objectives namely SMO-1, SMO-3, SMO-11, SMO-12, UMO-1, UMO-5 UMO-13 and UMO-15 as identified in the diagram 5.6.

Several such hierarchies can be developed by combining one or more of the information system security overall/over-arching goals (of confidentiality, integrity and availability) and one or more of the information system usability overall/over-arching goals (of efficiency, effectiveness and satisfaction). As such, given the appropriate business context and operational context, a computer based information system could have all of the information system security overall/over-arching goals (of confidentiality, integrity and availability) as well as all of the information system usability overall/over-arching goals (of efficiency, effectiveness and satisfaction). See figure 5.8 below for the computer based information system security and usability hierarchy with an information system security overall/overarching goals of confidentiality, integrity and availability and an information system usability overall/overarching goals of efficiency, effectiveness and user satisfaction.

Figure 5.8. Information System Security and Usability Hierarchy with **confidentiality**, **integrity**, **availability**, **efficiency**, **effectiveness** and user **satisfaction** as the overall/over-arching goals



As depicted in the above diagram 5.8., the combined information system security and usability hierarchy with the overall/over-arching information security and usability goals of confidentiality, integrity, availability, efficiency, effectiveness and user satisfaction can be achieved by focusing on all the information security and usability fundamental objectives as shown in tables 5.1 and 5.3 respectively. In addition, this hierarchy also highlights that all the security and usability fundamental objectives can be accomplished by meeting the associated security and usability means objectives as shown in tables 5.2 and 5.4 respectively.

Due to space limitations and to preserve the simplicity of the hierarchy, all the linkages between Security Fundamental Objectives, Usability Fundamental Objectives, Security Means Objective and Usability Means Objectives were not depicted in the above diagram 5.8.

5.7 Discussion

Security and usability related decisions that are made as part of the system development process are of complex in nature and require detailed and through analysis. As noted by Schoemaker and Russo (1993), "when a decision is truly important and complex, it may pay to conduct a more comprehensive assessment (Schoemaker and Russo 1993, p. 23)." Schoemaker and Russo (1993) further propose the pyramid of decision approaches, which consists of four different decision making method namely, intuitive judgments, rules and shortcuts, importance weighting and value analysis. Value analysis is placed on the top of the pyramid noting that it is the highest form of decision making approach which helps analyze the complex nature of decision making domain. Value analysis

helps the decision makers to understand the critical factors that are relevant for the decision making and to make an informed decision.

We argue that security and usability hierarchies discussed in the above sections fall in the category of value analysis and provide immense guidance to the business organizations' IT executives. By first selecting the overall/over-arching goals for security and usability, the decision makers can delve into the specific fundamental and means objectives that are relevant for the respective overall/over-arching goals of security and usability. Having such clear security and usability objectives will provide guidance and clarity in decision making.

5.8 Conclusion

The primary goal of this chapter to demonstrate how the security and usability fundamental and means objectives can be tailored to create security and usability hierarchies that are specific to a particular business or operational context. As noted in the previous paragraphs, the information system usability objectives derived from this research have been compared with the security objectives proposed by Dhillon and Torkzadeh (2006) to identify any security and usability objectives that are similar or conflicting with each other and arrange them in a hierarchical manner using AHP principles and concepts. Several combinations of security and usability hierarchies have been proposed and these proposed hierarchies attempt to achieve relevant information system security and usability goals.

Chapter 6 – Case Study Analysis

6.1 Introduction

In this chapter, a case of computer hacking was reviewed and discussed as to how several of the security and usability objectives identified in this research were directly or indirectly applicable in this published case. This chapter also discusses how some of the security and usability objectives identified in this research were not applicable to the published case as well.

Theory development is central to the organizational research (Eisenhardt 1989). Eisenhardt further notes that "an essential feature of theory building is comparison of the emergent concepts, theory, or hypothesis with the extant literature (1989, p. 544)". This means identifying the appropriate existing/published literature from a broad range of literature selection and comparing such existing/published literature to the emergent concepts by asking key questions such as the following:

- What was similar between the existing/published literature and the research that was attempting to build the theory?
- What were the contradicting aspects between the existing/published literature and the research that was attempting to build the theory?

For the purposes of this chapter, the emergent concepts were the research performed and documented in this dissertation. Specifically, the emergent concepts include the security and usability objectives. Comparing these emergent concepts to the existing/published literature such as the selected case study help build the theory and enhance the theoretical contributions of the current research of security and usability. More importantly, based on the information security and usability objective clusters as discussed in Chapter 5

above, we have made specific attempts to analyze and document which of these information security and usability objective clusters had not been met that potentially caused the security exposure.

The selected case for the comparison was first published in the Journal of Information Systems Security (Perez 2005) and is reproduced in full text in the Appendix-E.

As shown in Appendix-E, the computer hack case study, written by Sharon Perez, is a classic example of how easily the computer based information systems could be compromised with the readily available internet tools when appropriate security controls were not put in place because the system owners, system developers/administrators and system users were not in agreement with the system configurations. The case also illustrates that some of the minor disagreements such as the naming convention of the servers coupled with the back-end server and software technical limitations could lead to disastrous consequences. The tools and techniques used by the hackers illustrated in the case study were simple and readily available to anyone with a computer that had access to the internet. Such simplicity of available hacking tools highlights the pervasiveness and ever present danger of information security issues. Some of these information security issues also stem from the information system usability issues/disagreements as discussed below in the following paragraphs.

In addition, the chosen case was also a good example to illustrate what happens if the security and usability objectives of various stakeholders such as system owners, system developers/administrators and system users were not aligned. This case notes that disastrous consequences such as the computer based information system compromises as detailed in the case potentially could have been avoided. Furthermore, the case study

comparison supports and further validates the theoretical contributions of security and usability objectives identified in this research.

6.2 Case Overview

The case titled "Case of a Computer Hack" was based on the actual series of events that happened over a period of two years. The facts of this case were disguised as a hypothetical public university named as the Stellar University (SU) to protect the identity of the said university. The case describes a security incident that occurred at SU and the events that led to subsequent information security compromise. As discussed in detail in the following paragraphs, the information security compromise was partly due to the fact that the organizational culture did not allow for co-operation among various groups and departments and partly due to the power struggle among the various departments within SU.

The events that led to the ultimate security compromise at SU can be broadly divided into two categories namely internal and external events. Internal events were the events over which the SU had some control over to change or modify the outcomes and consequences. The case further discusses as to the specifics of what SU did or did not do to influence the internal events. And the external events were the events over which SU had no control except to prepare and to plan for any unforeseen consequences. External events were thrust upon the SU and the university had to just deal with them as these external events unfolded. The following two sub-sections discuss the internal and external events in detail. Afterwards, the actual security compromise and the remediation measures undertaken by the SU were discussed.

Internal Events

SU's network as well as IT infrastructure was diverse, varied and consisted of all the available and trendy technologies that were popular during that time frame. Since any department or university affiliated individual can set up a server, there was no central authority to understand all the changes happening in the environment. For example, when a new server was built and brought on to the SU network, if the server owner was not reporting to the network group, no firewall or specific port restrictions were put in place. In such an open and diverse environment, information system security was ensured only at the overall level without any specific security objectives or goals. Additionally, information security assurance was administrated and managed by diverse groups of people locally such as system administrators, system developers, system users and system owners. Ultimately, this type of server administration led to the practice of unskilled personnel managing the critical servers which were under their respective departments' control. To summarize, the following are some of the key aspects of the diverse computer and network environment established at SU over the several years of its existence:

- Computer servers could be setup by anyone in any department in the SU;
- Operating systems and applications consisted of all flavors and platforms;
- Network infrastructure used old and unsupported protocols and architectures as well as current protocols and architectures;
- Network perimeter firewall was in place with "deny all except" when explicitly allowed with specific firewall rules defined for outside access to the internal networks;

- IT purchases were not coordinated to ensure the hardware and software compatibility for network environment and ongoing maintenance by the internal staff and external vendors;
- Similar to the computing environment, corporate culture was diverse as well;
- Unskilled personnel were managing the security and administration of the servers;
- Intrusion detection systems were installed with minimal configurations;
- There were no processes and procedures in place for periodic review of the patches and implementation of relevant patches and upgrades to the software products;
- No policies or procedures were in place for the overall security management including passwords constraints, changing of passwords periodically, change of default passwords and server naming convention;
- Hardware and software hardening and benchmarks standards were not established to maintain consistency across the departments and the university;
- One server was created and allowed to be the most critical server for the entire SU IT environment by installing critical services relating to the domain control (Primary Domain Controller) and naming service (Windows Internet Naming Service) without provisioning for any backup of these critical services;
- No standard maintenance plans were implemented to the critical servers on any nodes of the network to keep the network up to date with patches and other software updates;
- No contingency plans were thought through and put in place to deal with the emergency situations;

- There were no periodic backup and recovery procedures implemented and there was no standard monitoring mechanism to ensure the implementation of such backup and recovery procedures.

To further elaborate on one of the critical aspects noted above, the organizational culture and stakeholder behavior was as diverse and as varied as the technology and the network environment. Few departments within SU worked cooperatively to share information as each department attempted to act as "tower of power" and to lobby for additional power by withholding the key information and being inflexible in any turf wars. Lack of cooperation and zero communication among the key stakeholders of the computer based information system users were the hallmark moments of the culture prevalent at SU.

The above listed internal events crated perfect environment for the security compromise that had happened at SU, which was discussed in the later part of this chapter.

External Events

Due to rapid changes in technology landscape and prevalence of Internet, inexpensive yet powerful tools such as DameWare products for network and system administration were also available for novice hackers ("script kiddies') to manipulate organizational networks such as SU. While the university had no control over such external events, it could have adopted to the changing technology environment by understanding the persistent security threats and vulnerabilities. Non-action on the part of SU could result in some consequences that could have been avoided by careful advance planning.

In addition, since SU is a public university, other significant external events that had significant influence on SU also included the changing financial difficulties of the province in which the SU operated. Due to deteriorating financial situation of the

province, the province decreased its financial contribution to all the public higher educational institutions in general and SU in particular. As such, these external events led to significant shift in SU management focus and re-organization to redefine and refine the roles and responsibilities of various departments in the university. These budgetary restrictions from the province also forced the SU to reduce the staff. Most of such staff reductions resulted in the elimination of IT infrastructure support personnel. These management and re-organization changes have only complicated the already complex technology environment and culture. Lack of sufficient funding and lay-offs across all the departments led to more chaotic and haphazard behavior of the system stakeholders at the SU. Stakeholders (system administrators/developers, system users and system owners) in various departments were frustrated with heavy workloads and constant changes in the procedures for many departments.

The above noted external events crated perfect environment for the security compromise that had happened at SU, which was discussed in the following paragraphs.

Security Compromise

Server_1, which was running on Windows NT 4.0 with service pack 5 and Internet Explorer 4 and hosted a slew of applications and functions as a primary domain controller, had been compromised on one fine February Monday morning. The hacker(s) gained access to the server by running a password crack program and using an authorized user credentials whose userid and password were the same and whose password had never been changed since userid was created. The hacker gained unauthorized access via TAPI2 service and then modified the Symantec Antivirus definitions file so that the unauthorized access would not tip off any IDS monitoring analysts or network engineers.

Afterwards, the hacker installed malware that would replicate itself when it was deleted by the system administrators subsequently.

On that specific Monday morning, the system administrator, who was accessing the server remotely and discovered that something was not right with the Server_1, contacted the system administrators in the computer centers to troubleshoot. However, after quick review of folders that were created, log activities and brief analysis of what might have happened, the system administrators concluded that something went wrong with the Server_1 as a potential hacker might have gained access to the server. However, it was unclear as to what exactly had actually happened to the server and the extent of the damage, if any, caused by the hacker. The SU IT administration decided to take interim steps to minimize the damage. The impacted server was disconnected from the network to prevent the spread of any damage due to the server compromise and until further review was conducted to determine the nature and extent of the security incident and its consequent damage to the IT environment.

Further investigation by both the SU administration as well as an outside forensic expert determined that, apart from the systemic weaknesses of non-standard policies and procedures and lack of appropriate patches and upgrades to the IT infrastructure, the weakest link in the server compromise was that the user of a particular system on the server had the same userid and password. This weakest link provided the hacker the much needed initial access to the server to manipulate and compromise the server_1 and the network. Due to this security breach, it was also assumed that the domain information on the server_1, which was functioning as the primary domain controller, could also have been compromised. The impact of the domain controller compromise

was huge since the entire authentication mechanism is dependent on the server_1 had to be reconfigured manually.

Remediation Measures

Due to the aforementioned security compromise on Server_1, the SU administration realized that several things within the computing network and IT environment had to be changed. Aside from the weakest link of the password policies and procedures, the SU administration also realized that SU's skills and experience in collecting, analyzing and deciphering the forensic evidence were insufficient and were not up to the industry standards for a public university like SU. As such, SU decided to implement several short-term and long-term remediation measures including, but not limited to, the following:

- Short-term Remediation Measures:
  - System administrators and outside forensic expert performed a series of steps to disable the Trojan and remove any infected files.
  - The malware was removed from the server and the outside forensic expert certified that the system was completely cleaned.
  - Password policies were modified temporarily to force all the users to change the passwords and this was done manually due to the existing system and technical limitations for all the users on the server. When the users log in to the respective applications next time, they were forced to change the password.
  - After the necessary measures of cleanup and restoration, the server_1 was brought back online for services and keep the applications in production to be available for users.

- Long-term Remediation Measures:
  - Symantec Antivirus process that was critical for real-time monitoring of the servers was added.
  - Temporary password policy changes were made permanent and the user listings were cleaned up to ensure that one user had only one user account.
  - Administrative shared accounts had been deleted by running special scripts any time the server reboots as this measure eliminates the possibility of the spread of the malware if installed on any server.

6.3 Case Analysis

As noted in the above paragraphs, the prima-facie evidence and analysis of the discussed case indicates that server compromise at SU was purely information security issue. While there may be a debate or disagreement as to what had caused the security compromise, there was no denying that the information system security at SU was impacted due to the security compromise on Server_1. However, it can be argued that the issues the SU faced in the above case had as much to do with the information system security aspects as with the information system usability aspects on the Server_1. In this section, the case was evaluated using the security and usability objectives. More specifically, in the following paragraphs, we evaluate how the case discussed in the section 6.2 above had either achieved or failed to achieve the security and usability objective clusters that were discussed in Chapter 5. If any of the security and usability objective clusters were missing in the discussed case, we provide specific reasons for the missing usability objective clusters.

Achieved Information System Security Objective Clusters

Of the nine security "means objective clusters" (see Table 5.1) and 16 security "fundamental objective clusters" (see Table 5.2), we argue that three security "means objective clusters" (see Table 6.1) and eight security "fundamental objective clusters" (see Table 6.2) were achieved in the SU environment and these are listed in the tables below:

Table 6.1. Achieved Information System Security - Fundamental objectives

Fundamental Objective (3 clusters)	
Enhance management development practices (SFO-1) e.g.: Provide employees with adequate IT training	**Provide adequate human resource management practices (SFO-2)** e.g.: Enhance individual/group pride in the organization
Enhance integrity of business processes (SFO-7) e.g.: Ensure that appropriate organizational controls (formal and informal) are in place	

Table 6.2. Achieved Information System Security - Means objectives

Means Objectives (8 clusters)	
Maximize awareness (SMO-3) e.g.: Ensure explicit understanding of organizational culture by individuals	**Optimize work allocation practices (SMO-4)** e.g.: Develop understanding of organizational and information use procedures
Ensure legal an procedural compliance (SMO-7) e.g.: Decrease the level of employer's tolerance for misuse of information	**Understand work situation (SMO-11)** e.g.: Minimize creation of disgruntled employees
Maximize fulfillment of personal needs (SMO-12) e.g.: Appreciate personal needs for job enhancement	**Understand individual characteristics (SMO-13)** e.g.: Interpret individual lifestyles
Enhance understanding of personal financial situation (SMO-14) e.g.: Eliminate personal benefit of sharing information with competitors	**Understand personal beliefs (SMO16)** e.g.: Minimize the need for greed in the organization

Missing Information System Security Objective Clusters

Of the nine security "means objective clusters" (see Table 5.1) and 16 security "fundamental objective clusters" (see Table 5.2), we argue that six security "means objective clusters" (see Table 6.3) and eight security "fundamental objective clusters"

(see Table 6.4) were missing in the SU environment for the **reasons** indicated along with the objective clusters in the tables below:

Table 6.3. Missing Information System Security – Fundamental objectives

Fundamental Objective (6 clusters)	
Develop and sustain an ethical environment (SFO-3) e.g.: Create an environment that promotes organizational loyalty **Reason**: With so many organizational changes, SU has failed to create an ethical environment.	**Maximize access control (SFO-4)** e.g.: Ensure physical security **Reason**: Physical security is decentralized and not maximized at SU.
Promote individual work ethic (SFO-5) e.g.: Minimize temptation to use information for personal benefit **Reason**: With budget cuts and lay-offs, the individual work ethic at SU is minimal.	**Maximize data integrity (SFO-6)** e.g.: Minimize unauthorized changes **Reason**: With decentralization and so many IT environments, there are no standard processes to ensure the data integrity at SU.
Maximize privacy (SFO-8) e.g.: Emphasize importance of rules against disclosure **Reason**: Due to the security breach, the security and privacy at SU are not maximized.	**Maximize organizational integrity (SFO-9)** e.g.: Create an environment of managerial support and solidarity **Reason**: SU has multiple departments that do not go along with each other causing a dent to the organizational integrity.

Table 6.4. Missing Information System Security – Means objectives

Means Objectives (8 clusters)	
Increase Trust (SMO-1) e.g.: Develop an environment that promotes a sense of organizational responsibility **Reason**: SU did not develop an environment that increases trust among the employees and the departments.	**Provide open communication (SMO-2)** e.g.: Create an open-door environment within all levels of the organization **Reason**: There was no open communication environment at SU.
Establish ownership of information (SMO-5) e.g.: Promote ownership in the organization **Reason**: SU never promoted or established any clear ownership, roles and responsibilities so users can take ownership.	**Clarify centralization/decentralization issues (SMO-6)** e.g.: Ensure a right balance between centralization and decentralization **Reason**: IT environment is decentralized without any clear strategic direction.
Improve authority structures (SMO-8) e.g.: Clarify delegation of authority **Reason**: SU has not made any conscious attempt to clarify the delegation of the authority.	**Ensure availability of information (SMO-9)** e.g.: Ensure adequate procedures for availability of information **Reason**: At SU, there were no standard policies or procedures to ensure the information security in general and the availability of data in particular.
Promote responsibility and accountability (SMO-10) e.g.: Clarify delegation of responsibilities **Reason**: SU has not made any conscious attempt to promote responsibility and accountability for any action or inaction of the employees.	**Ensure censure (SMO-15)** e.g.: Instill a fear of consequences **Reason**: There are no policies of procedures in place at SU that would deter any lax behavior of security on the part of the employees and the various departments.

Achieved Information System Usability Objective Clusters

Of the eight usability "means objective clusters" (see Table 5.3) and 16 usability "fundamental objective clusters" (see Table 5.4), we argue that two usability "means objective clusters" (see Table 6.5) and six usability "fundamental objective clusters" (see Table 6.6) were achieved in the SU environment and these are listed in the tables below:

Table 6.5. Achieved Information System Usability – Fundamental objectives

Fundamental Objective (2 clusters)	
Maximize ease of use (UFO-5) e.g.: Ensure ease of navigation through application	**Maximize user requirements elicitation (UFO-8)** e.g.: Ensure system functionality meets requirements

Table 6.6. Achieved Information System Usability - Means objectives

Means Objectives (6 clusters)	
Improve system search capability (UMO-3) e.g.: Ensure semantic based search features	**Maximize system efficiency (UMO-4)** e.g.: Ensure process fairness
Maximize data quality (UMO-5) e.g.: Enhance data integrity	**Maximize system esthetics (UMO-6)** e.g.: Enhance visualization of system security
Maximize task efficiency (UMO-14) e.g.: Maximize automation of manual tasks	**Maximize self-efficacy in training (UMO-15)** e.g.: Enhance system training quality

Missing Information System Usability Objective Clusters

Of the eight usability "means objective clusters" (see Table 5.3) and 16 usability "fundamental objective clusters" (see Table 5.4), we argue that six usability "means objective clusters" (see Table 6.7) and ten usability "fundamental objective clusters" (see Table 6.8) were missing in the SU environment for the **reasons** indicated along with the objective clusters in the tables below:

Table 6.7. Missing Information System Usability – Fundamental objectives

Fundamental Objective (6 clusters)	
Enhance system related communications (UFO-1) e.g.: Ensure exception reports go to management **Reason**: SU failed to establish the system relation communication between the different departments is smooth and congenial.	**Maximize system administration functionality (UFO-2)** e.g.: Enhance connectivity at affordable price **Reason**: SU had faced several financial difficulties and hence had to minimize the system administration functionality by cutting jobs and resources.

Improve data organization (UFO-3) e.g.: Ensure data archival functionality **Reason**: SU was unable to archive and backup the data on Server_1.	**Maximize system capability (UFO-4)** e.g.: Enhance application features Reason: SU had failed to enhance the system capability by installing patches and upgrades.
Maximize system integration (UFO-6) e.g.: Ensure functionality is designed into system **Reason**: SU did not maximize the system integration as the network and IT environment is as varied and diverse as it can be.	**Maximize standardization of system features (UFO-7)** e.g.: Enhance customizable interfaces **Reason**: SU systems are anything but standard across all the departments.

Table 6.8. Missing Information System Usability - Means objectives

Means Objectives (10 clusters)	
Clarify & improve system documentation (UMO-1) e.g.: Ensure easy access to system documentation **Reason**: It is unclear if SU has any standard system documentation.	**Maximize system access (UMO-2)** e.g.: Define role-based external access **Reason**: Access to the various systems at SU is not role-based and it dealt locally at the each application level.
Maximize database and system access (UMO-7) e.g.: Ensure web access to the system **Reason**: The access to several applications is uncontrolled as several users have multiple accounts.	**Maximize system integrity (UMO-8)** e.g.: Maximize system adaptability **Reason**: Systems and IT infrastructure at SU are decentralized and not scalable and adoptive to the changing technological and environmental needs.
Maximize disaster recovery (UMO-9) e.g.: Ensure data availability **Reason**: The domain data that is critical for authentication purposes on the Server_1 had never been backed up.	**Maximize system maintainability (UMO-10)** e.g.: Ensure hardware robustness **Reason**: The hardware that hosts Server_1 was not robust as there were several technical issues to upgrade even the naming conversion of the servers.
Maximize productivity (UMO-11) e.g.: Ensure automated password retrieval **Reason**: The productivity of the applications on the Server_1 is not productive as the password management is not automated.	**Maximize system reliability (UMO-12)** e.g.: Maximize process execution accuracy **Reason**: At SU, the Server_1 that was compromised was not reliable at all without any backup of the data and domain controller functionality.
Maximize security & privacy (UMO-13) e.g.: Decrease restrictiveness of system **Reason**: It is unclear if SU has any standard system documentation.	**Minimize system interruptions (UMO-16)** e.g.: Minimize system down-time **Reason**: It is unclear if SU has any standard system documentation.

Conflicting Nature of Security and Usability Objectives

As noted in the tables 6.3 and 6.4, six out of nine (66%) security "means objective clusters" (see Table 6.3) and eight out 16 (50%) security "fundamental objective clusters" (see Table 6.4) were missing in the SU IT environment. Additionally, as noted in the tables 6.7 and 6.8,six out of eight (75%) usability "means objective clusters" (see Table 6.7) and ten out of 16 (63%) usability "fundamental objective clusters" (see Table 6.8)

were missing in the SU IT environment. Based on these percentages, it can be concluded that majority of the security and usability fundamental objectives were missing from the SU IT environment.

The reason for missing a specific security or usability objective is different and depends on the nature and the type of the security and usability objectives. However, sometimes these reasons for missing a specific objective are not so direct and cleanly correlated to what was missing in security and usability. It is to be noted that some of the security and usability objectives were not achieved by SU for several other reasons, including the conflicting nature of certain security and usability objectives.

The successful implementation of one specific objective inherently prevents the adoption of another objective. Such conflict might arise between one security objective and another security objective or between one usability objective and another usability objective. In addition, such conflicting nature might also exist between one or more security objectives and one or more usability objectives.

For example, in this specific case, the usability fundamental objective of ease of use (UFO-4) was achieved which could be conflicting with the security fundamental objectives of maximizing access control (SFO-4), data integrity (SFO-6) and privacy (SFO-8). As such, it is to be noted that the conflicting nature of the security and usability are in inherent in the IT environment that do not allow certain security and usability objectives to be achieved in an IT environment. Hence, in order improve the security and usability at SU, the management had to make conscious decisions to choose the appropriate security and usability objectives to balance the security and usability in the IT environment.

6.4 Conclusion

As described in the above paragraphs, based on a thorough analysis and reasoning, we have identified that six security "means objective clusters" (see Table 6.3), eight security "fundamental objective clusters" (see Table 6.4), six usability "means objective clusters" (see Table 6.7) and ten usability "fundamental objective clusters" (see Table 6.8) had not been explicitly met in the case study of computer hacking at SU. While the reasons for missing objectives were detailed in the respective tables, conflicting nature of the objectives may also be the inherent reason for certain missing security and usability objectives at SU. SU management had to make conscious choices to balance the security and usability in the IT environment.

Chapter 7 – Conclusion

7.1 Research Overview

This research is based on Keeney's (1996) "value focused thinking' (VFT) approach. Firstly, the goal of this research was to identify the information system usability objectives using the VFT approach. The information system usability objectives were obtained by interviewing 35 research participants who were independent system developers and system users. This research was described in detail in chapter 4 above. As a result of this research, eight usability "means objective clusters" and 16 usability "fundamental objective clusters" were identified. Secondly, using information system usability objective clusters developed from this research as well as the information system security objective clusters developed by Dhillon and Torkzadeh (2006), a comparative analysis using the Analytic Hierarchy Process concepts was performed to identify the relevant hierarchies for information system security and information system usability.

Information system security hierarchies were categorized using the classical information system security definition of confidentiality, integrity and availability. Information system usability hierarchies were categorized using the popular usability definition that highlights the efficiency, effectiveness and user satisfaction.

7.2 Research Contributions

The research contributions of this dissertation can be divided into three major areas, namely theoretical contributions, methodological contributions and practical contributions.

Theoretical Contributions

In general, the two primary objectives of any research are fact finding and theory-building and (Wacker 1998). Wacker further argues that "good fact-finding research serves to provide fertile ground for subsequent new theory-building" (Wacker 1998, p. 371). We present that the facts found in the current research also form the basis for the theory building act. From a fact-finding perspective, in this research, we have found out what system users and system developers really value in terms of information system usability. These facts formed the basis for the theoretical contributions of this research. The theoretical contributions of this research are twofold. First, with the study of 35 research participants, we have inquired of their usability values and analyzed and summarized using the VFT approach the following eight usability "means objective clusters" (see Table 7.1 below) and 16 usability "fundamental objective clusters" (see Table 7.2 below):

Table 7.1. Information System Usability – Fundamental objectives

Fundamental Objective (8 clusters)	
Enhance system related communications (UFO-1) e.g.: Ensure exception reports go to management	**Maximize system administration functionality (UFO-2)** e.g.: Enhance connectivity at affordable price
Improve data organization (UFO-3) e.g.: Ensure data archival functionality	**Maximize system capability (UFO-4)** e.g.: Enhance application features
Maximize ease of use (UFO-5) e.g.: Ensure ease of navigation through application	**Maximize system integration (UFO-6)** e.g.: Ensure functionality is designed into system
Maximize standardization of system features (UFO-7) e.g.: Enhance customizable interfaces	**Maximize user requirements elicitation (UFO-8)** e.g.: Ensure system functionality meets requirements

Table 7.2. Information System Usability - Means objectives

Means Objectives (16 clusters)	
Clarify & improve system documentation (UMO-1) e.g.: Ensure easy access to system documentation	**Maximize system access (UMO-2)** e.g.: Define role-based external access
Improve system search capability (UMO-3) e.g.: Ensure semantic based search features	**Maximize system efficiency (UMO-4)** e.g.: Ensure process fairness
Maximize data quality (UMO-5) e.g.: Enhance data integrity	**Maximize system esthetics (UMO-6)** e.g.: Enhance visualization of system security
Maximize database and system access (UMO-7) e.g.: Ensure web access to the system	**Maximize system integrity (UMO-8)** e.g.: Maximize system adaptability
Maximize disaster recovery (UMO-9) e.g.: Ensure data availability	**Maximize system maintainability (UMO-10)** e.g.: Ensure hardware robustness
Maximize productivity (UMO-11) e.g.: Ensure automated password retrieval	**Maximize system reliability (UMO-12)** e.g.: Maximize process execution accuracy
Maximize security & privacy (UMO-13) e.g.: Decrease restrictiveness of system	**Maximize task efficiency (UMO-14)** e.g.: Maximize automation of manual tasks
Maximize self-efficacy in training (UMO-15) e.g.: Enhance system training quality	**Minimize system interruptions (UMO-16)** e.g.: Minimize system down-time

The second major theoretical contribution of this research is system security and security usability hierarchies as discussed in detail in chapter 5 above. The three the information system security hierarchies (of confidentiality, integrity and availability) and the three information system usability hierarchies (of efficiency, effectiveness and satisfaction) link the security and usability objectives obtained using VFT approach to the overall/over-arching goals of information system security and usability. The resultant practical contributions are discussed in the paragraphs below.

Methodological Contributions

"Information Systems Research can be classified as interpretive if it is assumed that our knowledge of reality is gained only through social constructions such as language, consciousness, shared meanings, documents, tools and other artifacts" (Klein and Myers, 1999, p. 69). Based on this definition, we argue that the research described in this thesis

can be considered as interpretive in nature because the research primarily used VFT approach to understand the values of information system users and developers who develop and/or evaluate the usability of an information system.

Weber (1987) argued that information system research would make progress by seeking a paradigm with a powerful theory behind it to drive specific research endeavors. Since the publishing of this seminal article that set the tone for the information systems research, several researchers have published numerous articles in various information system journals.

Methodologically speaking, this research uses the innovative and the most popular qualitative research methodology, VFT proposed by Keeney (1992). VFT assesses the "actual or potential consequences of action and inaction' (Keeney, 1992 p.6). This methodology has been used in the information security research over the last several years (Dhillon and Torkzadeh 2006; Mishra and Dhillon 2006). Successful implementation of this methodology in this research without obtaining any personal information of the research participants further validates the authenticity of the VFT approach and is a discrete data point in creating an information system research paradigm. The continued validation of the VFT methodology sets the tone for the future use of this research methodology not only in the information system research discipline, but in other relevant research disciplines as well.

Practical Contributions

The practical contributions of this research are manifold. Hitherto, when it comes to information system usability, there was little research on what was really valued by system developers and users. We argue that the results of this research that proposed

eight usability “means objective clusters” (see Table 67.1 above) and 16 usability “fundamental objective clusters” (see Table 7.2 above) are of immense help to the system owners, system developers and system users in real world while developing computer based information systems. These objective clusters highlight and help organizations that develop computer based information systems to focus on what is really critical from a system user or system developer perspective.

Moreover, as noted in the chapter 5, the three information system security hierarchies (of confidentiality, integrity and availability) and the three information system usability hierarchies (of efficiency, effectiveness and satisfaction) could be used in the system development processes by the organizations that develop computer based information systems. Depending on the context in which specific computer based information is used, its security and usability overall/over-arching goals can be simply defined and then using the individual information system security and usability hierarchies, the relevant fundamental and means objectives of information system security and usability can be identified. As such, these critical objectives can be incorporated into the requirements of computer based information systems that are being developed. Inclusion of system security and system usability requirements in the early stages of the system development ensures that appropriate goals of security and usability can be achieved with minimum cost of resources.

In addition, based on the published case analysis and reasoning, we have identified that 6 security “means objective clusters” (see Table 6.3), 8 security “fundamental objective clusters” (see Table 6.4), 6 usability “means objective clusters” (see Table 6.7) and 10 usability “fundamental objective clusters” (see Table 6.8) had not been explicitly met in

the case study of computer hacking. Such case analysis and the resultant contribution illustrate the practical application of the research findings.

7.3 Limitations

The primary limitation of this research is that the sample size of 35 research participants of system developers and system users is relatively small. Even though the population of the research participants is with independent system developers and system users, any general conclusions of the research across the varied and disparate information system developers and system users groups must be made with caution. The data collection methods of this research did not include collection of any personally identified information including the industry in which the research participants were then working or had worked previously. As such, the industry length and breadth of the research participants might not be representative of the information system landscape that consists of several industries.

Values are personal beliefs developed over time by the system developers and system users. These personal beliefs were influenced by the environment in which these individuals grow up, study, learn and work. Since all the research participants from North America, any generalization of the research conclusions to other countries and regions outside the North American continent may not be result in valid extrapolative conclusions.

7.4 Future Research Directions

This research used the basic concepts of Analytic Hierarchy Process (AHP) to develop information system security and usability hierarchies. However, by utilizing the advanced concepts of AHP such as matrices calculations for the information system security and usability hierarchies, further research can be conducted to clearly identify computer based information system alternatives that consist of the various security and usability objectives. By identifying various portfolios of information systems, a detailed study can be performed to understand the suitability of implementation of these computer based information system alternatives within a given organizational context.

In order to further enhance the theoretical contributions of this research, additional research of information system usability objectives elicitation can be performed with a broader sample of research participants of system developers and system users that includes research participants from different industries such as financial services, technology, industrial good, automotive, and others. Further research could also be performed with sample research participants of system users and system developers from different geographical regions such as Europe, Asia and African continent to thoroughly understand values that are culturally different from the North American continent.

In addition, there are multiple other opportunities for future research that includes research opportunities such as expanding the study to include more qualitative data when interviewing the research participants. Future research can also focus to develop and validate specific measurement variables for the eight usability "means objective clusters" (see Table 6.1 in chapter 6) and 16 usability "fundamental objective clusters" (see Table 6.2 in chapter 6).

Appendix-A: Survey Instrument

Version No - 1.1

Date: 04-06-2011

Determining Requirements for Information Systems Security and Usability

Research Information Sheet

Purpose of Research: The purpose of this research is to understand usability values within the context of an information system.

Approximate Time: It should take no more than 30 minutes to complete the interview.

Interview Questions: Interviewee will be asked to list values, feelings and wishes with respect of usability. After this, the interviewee will be interviewed to elaborate the deeper meaning behind the values listed. Please see Survey Instrument document for more details.

Note: Please note that no personally identifiable information is collected in this research and any data obtained will be anonymous and that interviewees can choose to stop participating in the interview at any time. For any additional information or questions, please contact Dr. Gurpreet Dhillon (gdhillon@vcu.edu) or Santa Susarapu (susarapusr@vcu.edu)

APPROVED

4/11/SA/26

Appendix-B: List of Raw and Cleaned-up Raw Values

#	Raw Values	Cleaned up Raw Values
1	Too restrictive	I wish the system is not too restrictive
2	My problem with that is when certain web pages blocked others got also effected which I use for my work	I wish the system does not block web pages that I use for my work
3	Value ease of use, user friendly, visually appealing, simplistic.	I wish the system is visually appealing
4	Connect with people via email, chat email and cell phone – International contacts, low cost	I wish the system helps me connect with international contacts via email, chat and cell phone for low cost
5	See all options and customized for each department so people do not	I wish the system has all options and customized for each department so people do not get confused
6	Like integrating data from the websites - like having UPS tracking number without having to go to UPS website	I wish the system integrates data from the websites
7	Like integrating data from the websites - like having UPS tracking number without having to go to UPS website	I wish the system integrates data from the websites
8	Ease of purchase – navigation is simple and quick	I wish the system allows navigation and purchase of an item easier and quicker
9	Be able to clarify and understand options	I wish to be able to understand and clarify options
10	911 location giving nearest street plus latitude and longitude (for off road)	I wish the system can give location, latitude and longitude options
11	Language features (Arabic, English)	I wish the system has multiple language support
12	Training	I wish there is training for the system
13	Security questions/image	I wish the system has security questions/images
14	Ability to exchange data with Meditech system	I wish the system has the ability to exchange data with Meditech system

15	Never ever allow over-writing of base files unless specifically notifying and asking the user	I wish the system does not overwrite base files only after notifying and asking the user
16	My problem with that is when certain web pages blocked others got also effected which I use for my work	I wish the system does not block web pages that I use for my work
17	Ease of password recovery	I wish the system allows to recover passwords easily
18	Cryptic error messages	I wish the system does not give cryptic error messages
19	Clarity/color/brightness	I wish the system has clarity/color/brightness
20	History and archive of my past purchases, interests, etc. to make recommendations	I wish the system keeps the history and archive of my past purchases, interests, etc. to make recommendations
21	Back up of data	I wish the system backs up data
22	Same as above – remove flaws during data transfer from one page to another.	I wish the system automatically removes any flaws during data transfer from one page to another
23	Alt route suggestions	I wish the system has alternative route suggestions
24	A user manual must be available for ease of use and to answer questions	I wish a system user manual is available for ease of use and to answer questions
25	eBay is not responsible for any transaction (Easy, but not responsive)	I wish the system is responsive and responsible to transactions
26	Ideally windows should not have tried to copy Apple with Vista	I wish the system should have been design from scratch without copying from other systems
27	Large screen	I wish the system has large screen
28	Appearance – web page needs to look updated or modern to feel more confident in system. Pictures are comforting.	I wish the appearance of the system is better
29	Ability to go back to most recent page	I wish the system has the ability to go back to most recent page

30	Keeps me organized	I wish the system keeps me organized
31	Not too sensitive to environmental changes. Value more durability	I wish the system is not too sensitive to environmental changes and is durable
32	Sometimes you get a good deal	I wish I get a good deal
33	Type basic information and get faculty resource/information	I wish the system lets me type basic information and get faculty resource/information
34	Value simplified web-page appearance	I wish the web pages are simplified in appearance
35	Give me what I want and use is not what you want to give me	I wish the system give me what I want and use is not what you want to give me
36	Data remembering (payment methods, addresses) (Target.com does remember payment info.. but Amazon.com does not remember multiple shopping info.)	I wish the system remembers my payment methods, addresses, etc.
37	Also using radio systems and other hardware that appear to be old and out of date	I wish the systems and hardware are not outdated
38	Everything laid out – easy to be seen – visual, clear and organized	I wish the system lays out features clearly, visually and organized
39	Achievement of goals leads to my expected outcome	I wish the system helps me achieve my goals with expected outcomes
40	Could make do with another but not	I wish the system is indispensable
41	Tools (are categorized in a way that takes you there with common sense)	I wish the system tools are categorized in a way that takes you there with common sense
42	Buy - sell stocks	I wish the system allows to buy and sell stocks
43	Value ease of use, user friendly, visually appealing, simplistic.	I wish the system is user friendly
44	Long waiting time (i-pod charger reach after 1 month, but prince is very less)	I wish there is no waiting period to receive the product
45	Unlimited storage / archive	I wish the system has unlimited storage/archive

46	Easily manipulative and interpretable output/results – clear results that can be used effectively.	I wish the system generates output/results that could be easily manipulated and interpreted.
47	The Help Button should launch you to a very specific part of the documentation based on your query. It should never be online docs (who is connected when you need help!)	I wish the system's help should be context specific and should not be generic online documents
48	Clear process visually – no confusion on how to do the next step	I wish the system displays the process visually without any confusion as to how to do the next step
49	Web base	I wish the system is web based
50	A sample use of the tool should be provided. i.e. provide a set of inputs, and setups so that the user can run the program once without having to know it in order to see it at work and understand how it does things. If there is lots of different functionality, provide one example per functionality type.	I wish the system has the ability to show potential users of the sample use without any complex inputs and set ups
51	More use of sense/voice and less of keyboard to save time	I wish the system users more of sense/voice and less of keyboard to save time
52	Closing the month AP – software let you go back and make changes to revenue which requires too much work	I wish the system has the ability go back and make changes to revenue which requires too much work
53	New system changes	I wish the system enhancements are better communicated
54	Detailed database large	I wish the system is supported with detailed and large database
55	We are also using MS system for scheduling. And it is really hard to update according employees' special needs	I wish the system is easy to update according to employees' special needs

56	On/off road options/data	I wish the system has multiple options for data
57	Improve service and reliability	I wish the system has improved service and reliability
58	Hours I can access the information	I wish the system allows me to access my information
59	Consistent look across components	I wish the system has consistent look across all components
60	Speed – how quickly wanted information can be accessed and provided.	I wish the system allows information access quickly
61	I would like to make special effort to understand instructions	I wish the system's instructions are easy to understand
62	Large buttons when driving mode	I wish the system has large buttons to use when driving
63	Help desk or user manual easily accessible	I wish the system has help desk or user manually easily accessible
64	People lie about product condition	I wish people who sell products online do not lie about production condition
65	Blackboard: order of icons, appearance, search people	I wish the system is organized
66	Live traffic data interface	I wish the system has live traffic data interface
67	Successful completion, efficiency in daily tasks (workforce reduction), real time reports, smoother operation, automatic controls	I wish the system has several features including successful completion, efficiency in daily tasks (workforce reduction), real time reports, smoother operation, automatic controls
68	Encrypts (whenever visiting Korean sites)	I wish the browser encrypts whenever I visit Korean sites
69	Would like for GPS to provide crash feedback, be able to call for help	I wish the system provides crash feedback and calls for help
70	Upgrades should happen (or at least announce themselves) automatically	I wish the system upgrades happen automatically
71	Updated info should be sent as messages eg. Email alerts to notify users.	I wish the system sends updated messages and notifications for users
72	Limit staff visibility	I wish the system limit staff visibility

73	Not too many pop-ups or stop gap ads that slow down the process when trying to go to a different page or through checking out	I with the system does not have too many pop ups or stop gap ads that slow down the process when trying to go to a different page or through checking out
74	Collaboration with easy to use tools to help coordination efforts	I wish the system has better collaboration with easy to use tools to help coordination efforts
75	Multiple sign ins – more secure	I wish the system has multiple sign-ins for more security
76	Having the option of saving all passwords along with the master password	I wish the browser has the option of saving all passwords along with the master password
77	Having the option of saving all passwords along with the master password	I wish the browser has the option of saving all passwords along with the master password
78	Having the option of saving all passwords along with the master password	I wish the browser has the option of saving all passwords along with the master password
79	Ease to use, convenient	I wish the system is easy to use and convenient
80	Sorting and query features with data must be available	I wish the system allows sorting and query features to manipulate the data
81	Speed	I wish the system has speedy response
82	Fonts breaking up	I wish the fonts in browser are not displayed as breaking up
83	For in dash a crash sensor feedback like onstar	I wish the system has a crash sensor for feedback like onstar
84	Ease to navigate	I wish the system is easy to navigate
85	Access – able to understand the interface	I wish the system interface is understandable
86	Installation should be completely automated and launch at least the basic version/view.	I wish the system installation is automatic to launch at least the basic version/view
87	Ease of operation	I wish the system is easy to operate

88	Not require prior training / less tedious	I wish the system can be used without any prior training and the system is less tedious
89	Main menu with many search options	I wish the system has many search options
90	Successful completion, efficiency in daily tasks (workforce reduction), real time reports, smoother operation, automatic controls	I wish the system is efficient
91	There should be at least 2 ways to accomplish the same thing. This could be menu-based vs. key-based. Or 2 different ways through a menu. People's minds are set up differently. Accommodate them.	I wish the system allows to accomplish the same task in multiple ways to allow different types of users and their learning abilities
92	Good security – flexibility needed	I wish the system has good and flexible security
93	Different standards for different functionalities	I wish the system did not have different standards for different functionalities
94	Multi functional currency – for international firm	I wish the system has multi functional currency features
95	Correct interpretation of my intent – I want exactly what I want, nothing more.	I wish the system interprets my intentions correctly
96	Mouse be able to click on it,	I wish I could the mouse
97	Privacy - Windows multiple users, identify theft	I wish the system has identify theft protection
98	Single system with same system	I wish the system consists of all components
99	Smart system	I wish the system is smart
100	Interconnectivity between components	I wish the system provides interconnectivity between components
101	Adequate reports – ability to export	I wish the system has the ability to export and generate adequate reports
102	Would like to access accounts through smart phone	I wish to access accounts through smart phone
103	Securing data with multi level security is important with data – lock out/s at session end is good	I wish the system secures the data with multi level security and automated lock outs and session ends

104	Able to load on more than one computer for quick transfer	I wish the system is able to load on more than one computer for quick transfer of tasks
105	Order as credit cards	I wish the system allows to manage my credit cards
106	Privacy - Windows multiple users, identify theft	I wish the system has privacy with multiple users' use
107	Accurate execution – sometimes not very dependable	I wish the system executes accurately
108	Security of credit card information (Purchasing mine)	I wish the system protects the security of credit card information
109	Safety	I wish the system is safe to use
110	Ease of navigation – finding what I need fast and with ease. No difficulties involving not being able to figure systems working process out	I wish the search and navigation features of the system allow me to find the information faster
111	Instant support	I wish the system has instant support
112	Value balance between protecting themselves from liability and be able to maintain functionality while reviewing. Locks out a little too much	I wish the system values functionality and does not lock out too much
113	Successful completion, efficiency in daily tasks (workforce reduction), real time reports, smoother operation, automatic controls	I wish the system processes real time transactions and operates smoothly
114	Easy to user resources – online for help support	I wish system provides online user resources for help support
115	Ease of research, accessing journals from home	I wish I could access the data from the system from home
116	Safety is extremely important	I wish the system safety is important
117	On Amazon.com, no need to login (saves time)	I wish the system does not require any login to save time

118	Verbal interface with good speech recognition	I wish the system has verbal interface with good speech recognition
119	Adaptability	I wish the system is adaptable
120	More convenience for section of parts. Allow to assign functionality to more easily	I wish the system can assign functionality easily and conveniently
121	Administration of features	I wish the system has administration features
122	Clarity – shows menus in clear way - does not use funny terms. Unsure…	I wish the menus in the system have clarity
123	Ability to enter post closing transactions	I wish the system has the ability to post closing transactions
124	Just worked on making it more efficient	I wish the system is more efficient
125	A well connected system (be able to email to oneself from outside search engines)	I wish the system is well connected (be able to email to oneself from outside research engines)
126	Owner should dictate access administration levels	I wish the system owner dictate the access administration levels
127	Ease of use and clear to save time and increase performance	I wish the system increases performance
128	Site or system should not be too slow – anything , flash, html – Don't care as a user, as long as it is fast	I wish the system is faster
129	Sometimes not reliable as item does not reach me always (a buy, not reach)	I wish the delivery of the items ordered is reliable
130	User must have reporting features to meet needs	I wish the system has reporting features to meet the needs
131	Google chrome the history is kept. Save time. Google is not secure. Security is a problem. Google has…	I wish the system is secure
132	Security / Privacy - both no access	I wish the system has security and privacy
133	Can be synched with other systems and new system	I wish the system can be synched with other and new systems

134	As far as EMS system is concerned, would want a more user-friendly version, more accurate with schedules, more flexible for users.	I wish the system is user friendly, with better version control and accurate and flexible
135	Clarity/color/brightness	I wish the system has clarity/color/brightness
136	At work our network is limited to certain web pages because my boss thinks it decreases the productivity.	I wish the system allows all web pages to increase my productivity
137	Utility is poor = data not able to be pulled	I wish the utility of the system is not poor
138	Value balance between protecting themselves from liability and be able to maintain functionality while reviewing. Locks out a little too much	I wish the system values functionality and does not lock out too much
139	Collaboration	I wish the system promotes collaboration
140	Membership interaction	I wish the system has membership interaction
141	Wishes: bunch of things, but need to do little better way	I wish the system does things in a better way
142	Done by the company applying to - no redirecting to other vendors	I wish the system does not redirect me to some other vendors
143	eBay itself should involve a risk	I wish the system involves some risk
144	No user maximum.. unlimited users (less licenses) to prevent purchases of licenses	I wish the system has no maximum user limitation.
145	Fewer number of clicks	I wish the system has fewer number of clicks
146	No form	I wish there are no forms
147	Time constraint is a potential issue	I wish the system has no time constraints

148	It should work on the majority of cases/types directly out of the box with no special configurations or customizations. Someone with no experience with the tool (how would they choose a customization) should be able to get it to work immediately on their basic problem.	I wish the system has no major configurations or customizations
149	The system must have no delay to save time	I wish the system avoids delays
150	Being able to visit sites without any interruptions (pop ups and cookies)	I wish the browser allows me to visit sites without any interruptions
151	The system must not freeze to avoid delays	I wish the system does not freeze
152	Ability to download without interruption	I wish the system has the ability to download without any interruption
153	-Different platforms	I wish the system does not have too many different platforms
154	Security and firewall features must be available to prevent increases and hacking	I wish the system security and firewall features must be available to prevent increases and hacking
155	Longer periods of pause	I wish the system does not have longer periods of pause
156	Value cheaper/easier upgrade options	I wish the system has cheaper and easier upgrade options
157	Training – most performed as open	I wish the system has less training
158	Value balance between protecting themselves from liability and be able to maintain functionality while reviewing. Locks out a little too much	I wish the system values functionality and does not lock out too much
159	See all options and customized for each department so people do not	I wish the system has all options and customized for each department so people do not get confused
160	Self-to-do model and not professional assistance	I wish the system has self-to-do model without any professional assistance

161	If your tool needs a developer's forum (for setup, not for here's my new neat trick with it), or a user's forum, you've failed in usability.	I wish the system can be used without interacting with the developer's or user's forum
162	Windows 7 seems to be an improvement	I wish the system shows improvement from previous versions
163	Identify thefts to be prevented (by credit card)	I wish the system prevents the identity thefts
164	The process must be simple to avoid stress and training, which is to save time	I wish the system saves time
165	Easy to use	I hope the system is easy to use
166	Systems that everyone uses (popular – easier to get questions)	I wish the system is popular and everyone uses so it would be easier to get questions answered
167	User interface is rich, pleasant to the eye	I wish the system's user interface is rich and pleasant to the eye
168	Value more icons	I wish the system values more icons
169	Pay bills	I wish the system allows to pay my bills online
170	Value faster speed	I wish the system is speedy
171	Be able to trade through online banking accounts	I wish I am able to trade through online banking accounts
172	Value language options	I wish the language options are valued
173	Bluetooth interface	I wish the system interacts with Bluetooth interface
174	Value signal reception	I wish the system has good signal reception
175	Would like it to be more affordable/extensive	I wish the system is more affordable and extensive
176	Value clear/big screen, readable, very audible	I wish the system has clear big screen with readable and audible quality
177	Speech recognition has to be top-notch	I wish the system has top notch speech recognition
178	Value alternate traffic suggestions, more so for longer trips	I wish the system has alternative route suggestions, more so for longer trips

179	Would like the development of voice recognition software	I hope the development of voice recognition software is better
180	Library: Few clicks – how you find journals …. volumes.. issues, - Ease of use	I wish the system is easy to use
181	Would like less effort while using library resources	I wish the system is usable with less effort
182	Generalized research, be able to type a few words and get accurate results (like Google)	I wish the system lets me type a few words and get accurate search results
183	A more visible search engine	I wish the search engine on the website is more visible
184	Value ease of use, user friendly, visually appealing, simplistic.	I wish the system is easy to use
185	Value ease of use, user friendly, visually appealing, simplistic.	I wish the system is simplistic
186	VCU related web pages, specific search engine	I wish the system allows me to use specific search engine
187	Cannot fully utilize VCU library web pages, would like to be able to do so	I wish I could fully utilize web pages
188	EMS system is not very user friendly, not very clear. Would like to research more while at work	I wish the system is user friendly and clear to help me to do research at work
189	Korean websites, Firefox blocks, Korean language, fast to download	I wish the system allows me to down load faster
190	Firefox is scanned, but I want to save it, it is not that like Internet Explorer	I wish the system allows Korean language websites
191	Speed of moving to the next page	I wish the speed moving to next web page is faster
192	Good search ability	I wish the system has good search ability
193	Shopping – ability to buy without logging in	I wish the system has the ability to buy without logging in
194	No remember of password	I wish I do not have to remember passwords
195	Size of presentation on page; Go to whole page; 20 results on page should be seen	I wish the search results display contains 20 results per page

196	Ease of finding the right item (eg. Ask for iPod, it not gives Android) (books purchase; easily and low priced)	I wish the system helps me find the right item easily
197	Ease of browsing (easily related links)	I wish the system makes the browsing easy
198	Less complicated website (finds easily)	I wish the website is less complicated
199	Quick answer	I wish the system provides me with quick answers
200	Cookie allowances (Korean fonts)	I wish the browser cookies allow Korean Fonts
201	Better add-ins download from Firefox; newly add in	I wish the browser has better add-ins
202	Auto spelling correction (writing helpful with a paper)	I wish the browser has the auto spelling correction
203	Stylish compared to other internet operating system	I wish the browser is stylist compared to other internet operating system
204	Ease of use and clear to save time and increase performance	I wish the system is easy to use and clear
205	The system must have exporting and importing capabilities to meet needs	I wish the system has exporting and importing capabilities to meet needs
206	A user manual must be available for ease of use and to answer questions	I wish a system user manual is available for ease of use and to answer questions
207	Size of system must be large data to be entered	I wish the system allows large data to be entered
208	No redundant password entry	I wish the system has no redundant password entry
209	Visit sites without false denied access	I wish the system allows me to visit sites without false denied access
210	Visit sites without false denied access	I wish the system allows me to visit sites without false denied access
211	Mobile device re log in VCU wifi every time	I wish the mobile device would not ask for re-logging in to VCU wifi every time
212	Security of personal information (passwords protection) but not too much	I wish the system secures the personal information
213	Speed (from screen to screen)	I wish the speed from screen to screen is faster

214	Sophisticated (up-to-date technology) – confident in system	I wish the system is sophisticated
215	Office + Windows vs. MAC – People need to be able to open	I wish system is interoperable
216	Systems that everyone uses (popular – easier to get questions)	I wish the system is popular and everyone uses so it would be easier to get questions answered
217	Password protection is good but can be too much to remember	I wish the I do not have to remember the passwords
218	Want remote feature security without hassle	I wish the system has remote feature security without hassle
219	Speed was not … feedback, on hurry	I wish the system is faster
220	Tools bar should be organized so does not waste time search	I wish the system tool bars should be organized so the I do not waste time searching
221	Easy to search for	I wish the system is easy to search features
222	24 hrs access to system support	I wish I have 24 hrs access to the system support
223	H&R System on the side, fairly new one, Dos based system, frustrating, mouse does not work, have to use key board	I wish the system is less frustrating
224	Support or search process for complicated work issues save time by not selecting screens	I wish the system support or search process for complicated work issues saves time
225	User friendly – most important because all levels need to use. Lower level people struggle and slowing down	I wish the system is user friendly
226	Controls – more autonomous internal controls	I wish the system has more autonomous internal controls
227	Access – home / work – for after hours or sick	I wish I could access the system from home
228	Support – very needed when starting - very important	I wish the system has support
229	Speed	I wish the system is faster

230	Promote efficiency – better than before, but not in every department	I wish the system promotes efficiency
231	Speed – running system for work and do too much at once and is slow. Slows work pace.	I wish the system is faster
232	Navigation ease – Website, market research, how hard to search, data buried, not simple, very scattered, are loaded	I wish the navigation and search ability in the system are easier
233	Integration across all divisions and operations – multiple divisions, but lack of consolidation and has to be input false codes. Loss of time.	I wish the system integrates and consolidates across all divisions and operations
234	Speed – screen to screen is first, step, jump around more than necessary	I wish the system is faster when going from screen to screen without jumping around
235	Less security prompts – DoD – DPACS separated SAP so could login separately	I wish the system has less security prompts
236	Easier to add absent info – Home to add codes monthly functional. So he can add codes without	I wish the system allows to add absent information easily
237	More intuitive user interface	I wish the system has more intuitive user interface
238	System is outdated in mid 90s. Set up from DOS but very out dated and more modern life.	I wish the system is more current
239	Ease of access – how easy it is to enter, use and locate al the needed information.	I wish the system is easy to use when entering data and locating needed information
240	Security – safety of data and personal information must be upheld at all costs. confidential to company, clients data	I wish the safety of confidential data and personal information is upheld at all costs.
241	Steps are clear and concise (for end point)	I wish the system has clear and concise steps
242	All of my questions answered right when I have them	I wish the system answers all my questions

243	Efficiency – how much time it takes to input and amount of return on the input.	I wish the system improves efficiency and processing time
244	1 hour - I want something worth my time	I wish the system saves my time
245	Is my information safe?	I wish my information is safe in the system
246	Is the company reliable?	I wish the system vendor is reliable
247	Is the product of good quality?	I wish the system quality is good
248	After signup – 1 – 2 – 3 – 4 – etc.	I wish there are no multiple signups
249	Ease of purchase	I wish it is easy to buy using the system
250	Shean q – in and out – fast and smooth	I wish the system is works faster and smoother
251	Intuitive system	I wish the system is intuitive
252	Less complicated the better	I wish the system is less complicated and better
253	Time values of money	I wish the system values time value of money
254	Smooth interface	I wish the system has smooth interface
255	Easy to navigate and understand	I wish the system is easy to navigate and easy to understand
256	Site is clear	I wish the system is clear
257	Uploading of documents (resume and cover letter)	I wish the system has the documents uploading feature
258	Identification of personal info from the resume (Education, career experience, certification)	I wish the system identifies my information
259	Ease navigation (separate tabs for each step)	I wish the system is easy to navigate and has separate tabs for each step
260	Log back in feature to in order to make changes	I wish the has the log back in feature to make changes
261	You can go back to previous steps	I wish the system can take me back to previous steps
262	How quick? – 5-10 if it can recognize your info	I wish the system can recognize my information
263	Should not make you think too hard	I wish the system does not make me think too hard
264	Best use of my time	I wish the system makes the best use of my time

265	System should be intuitive	I wish the system is intuitive
266	Less complicated, the better	I wish the system is less complicated
267	Also I use to help maps and search engine and web browse	I wish the system is useful to help find maps
268	Also I use to help maps and search engine and web browse	I wish the system is search and web browsing
269	Google the internet got everything. It will be nice to have a software where it shows everything.. hard to find everything .. so much stuff in	I wish the system can help me find things I am looking for
270	It is difficult to know all the applications that Google has. Therefore, not using Google as good as I could.	I wish the system can help me find all the applications
271	The web browser gives problems sometimes when you make many things at the same time. Save time.	I wish the system does not freeze/crash when multiple functions are performed to save time
272	Google chrome the history is kept. Save time. Google is not secure. Security is a problem. Google has…	I wish the system keeps the history intact.
273	Speed – does not like technology	I wish the system is speedy
274	Simple - wants ease of use – does not like technology – not IT systems	I wish the system is easy to use
275	Only necessary options – do need extra features	I wish the system has necessary and additional features
276	Clarity/color/brightness	I wish the system has clarity/color/brightness
277	Speed of data transfer	I wish the system enables speedy data transfer
278	Do not want to go through 10 pages to make a purchase - information should be easily accessible . eg. FAQ page – click not helpful – key word search is better	I wish the information in system is easily accessible

279	Different sites have different error formats – standardized error messages, more user friendly – way it is displayed have friendly error message that tells you what's wrong.	I wish the error messages are standardized
280	Error message – click and directed straight to held of error – No multiple options on initial error page	I wish the system gives error messages straight forward
281	Eg. Hotmail, Gmail login 0 different ways of showing data, for eg. Post back vs. instant screen accommodation for data display. Should be standardized. Some systems are too "bulky'. Prefer a more manageable amount of data on screens or pages.	I wish the system standardizes data and application display
282	Consolidation of steps – speed of process	I wish the system consolidates the steps to speed up the process
283	Clear navigation tools and search bars to find what I want	I wish the system provides clear navigation tools and search bars to find what I want
284	Based on easy navigation of AMazon.com , eg. Category and search bar – being able to remember user to make secondary visits easier.	I wish the system has easy navigation and other features to remember user preferences to make secondary visits easier
285	Eg. Ad pop ups – close windows to get to new pages – should be able to navigate across pages. Consolidate check out data – prefer having all info on one page – view all	I wish the system has easy navigation and consolidates the check out data
286	Tools important – auto completed – drop down menu are good relate or narrow down to previously viewed pages of searches – must be visually clear and simple	I wish the system is visually clear and simple

287	Ties into last topic – website needs to be secure about past purchases and credit card data but should be able to remember and archive data for easy recurring use.	I wish the system is secure and remembers, yet protects all past purchases and credit card data
288	Speed	I wish the system is speedy
289	Easy to navigate	I wish the system is easy to navigate
290	Ability to electronically post from general ledger	I wish the system has the ability to electronically post from general ledger
291	Interface speed, per click, get stuff done without unnecessary intervals	I wish the system has speedy interface and get stuff done without unnecessary intervals
292	Easy system accessibility and easy to get from point A to point B	I wish the system has easy system accessibility and easy to get from point A to point B
293	Running on two different systems with no data transfer capability - data communication between systems is important	I wish the system can run on one consolidated system
294	Running on two different systems with no data transfer capability - data communication between systems is important	I wish the system has better data communication
295	Based on 4, be able to transfer data for convenience	I wish the system has the ability to transfer data for convenience
296	Speed	I wish the system is speed
297	Menu of options (easy to locate materials)	I wish the system has menu options (easy to locate materials)
298	Up-to-date information/real time	I wish the system is up-to-date with information in real time
299	Email alerts	I wish the system has email alerts
300	Faster the better, loading speed is important – more of the page speed than actual data change speed	I wish the system is faster with speedy loading of data

301	Use friendly pages – navigation easy per page – eg. BOA page graphically or list drop down works better than search bars – don't like additional windows.	I wish the system has user friendly pages
302	Use friendly pages – navigation easy per page – eg. BOA page graphically or list drop down works better than search bars – don't like additional windows.	I wish the system has better navigation
303	Use friendly pages – navigation easy per page – eg. BOA page graphically or list drop down works better than search bars – don't like additional windows.	I wish the system graphically lists or has drop down menus rather than additional pop-up windows
304	Updating data more when possible – real time changes important – eg. Tax forms available as fast as possible	I wish the system provides real-time information as fast as possible
305	Single sign on for easy of access	I wish the system has single sign on for easy of access
306	Flexibility in reporting – create custom reports	I wish the system is flexible in reporting and creating custom reports
307	Centralized reporting	I wish the system has centralized reporting
308	Shortest navigation	I wish the system has shortest navigation
309	Customizable naming of options	I wish the system has customizable naming of options
310	Security flexibility to provide additional access	I wish the system has security flexibility to provide additional access
311	In system documentation for understanding functions	I wish the system has documentation to understand the functionality
312	Clean interface for easy readability	I wish the system has clear interface for easy readability
313	Simplicity	I wish the system is simple
314	Access across network – controlled access is good –	I wish the system controlled access across network

315	Security is highly important	I wish the system considers security as highly important
316	Works provides easy access to tool to manage products	I wish the system provides easy access to tools to manage products
317	Easy – consistency between 3 independent pieces	I wish the system is easy and consistent
318	Fairly intuitive – simple –	I wish the system is simple and fairy intuitive
319	Consistent interface – migrate between gap	I wish the system has consistent interface and has no migration gaps
320	Likes (-See sales figures, -Spec sheets -Can track orders, -Stored quotas, -Contact lists)	I wish the system features all my likes
321	Track orders	I wish the system can track orders
322	Ship dates	I wish the system can display ship dates
323	Highly security	I wish the system has high security
324	Web based, can do from anywhere	I wish the system is web based and can be accessed from anywhere
325	Good speed	I wish the system has good speed
326	Accessible	I wish the system is accessible
327	Data available, just not user friendly	I wish the system makes the data available
328	Data available, just not user friendly	I wish the system is user friendly
329	Multiple sign ins – more secure	I wish the system has multiple sign-ins for more security
330	-So many sign ins	I wish the system did not have too many sign-ins
331	-Times out too quickly	I wish the system does not time out too quickly
332	Interface = no training – intuitive	I wish the system has better interface
333	Interface = no training – intuitive	I wish the system can be understood with no training
334	Interface = no training – intuitive	I wish the system is intuitive

335	Not branded, no core values – some branding in customer area	I wish the system has a brand and core values in the customer area
336	More customer friendly –	I wish the system is more customer friendly
337	Forget password - Have to go through IT to get password	I wish the system has a feature to retrieve passwords without going to IT
338	Values: simple, familiar design	I wish the system is simple with familiar design
339	Compatibility with most products / systems	I wish the system is compatible with most other products/system
340	XP had basic design (less crashes)	I wish the system has basic design with less crashes
341	Growing up with IT	I wish the system is evolutionary
342	Confusing otherwise	I wish the system is not confusing otherwise
343	Compatible with other applications	I wish the system is compatible with other applications
344	Develop own advantages	I wish the system has advantages
345	Improve efficiency	I wish system improves the efficiency
346	Not best, but familiar robust	I wish the system is familiar but robust
347	Use most: My computer, Documents, Pictures, Navigation from and within folders	I wish the system provides easy access to most used folders
348	Cheapest options to manage email vs. exchange server, Lotus Notes, Dominos	I wish the system is inexpensive to manage
349	Not many like it free	I wish the system is inexpensive
350	Web apps customizable wigits	I wish the system has web apps with customizable wigits
351	Security is not very important because of type of email	I wish the system has security features based of the type of email
352	Company cheaper option	I wish the system is inexpensive
353	No other services or products support	I wish the system supports other services

354	Other systems are better tested of core features	I wish the system has better core features
355	Easy search of emails	I wish the system has easy email search features
356	Simple upload/download of attachments	I wish the system makes it simple to upload/download of attachments
357	Simple internal user lookup	I wish the system has simple internal user lookup
358	Anywhere / anytime accessibility	I wish the system is accessible anywhere / anytime
359	Sync with mobile devices	I wish the system syncs with mobile devices
360	Consistent always on	I wish the system is consistent and reliable
361	Easy organization	I wish the system is makes it easy to organize
362	Fast email service	I wish the system provides faster email services
363	Multiple email aliases selection	I wish the system allows multiple aliases selection
364	Calendar sharing/viewing	I wish the system allows calendar sharing and viewing
365	Strong self-help support	I wish the system has strong self-help support
366	Password convention – changing	I wish the system password convention is changed
367	Easy of maneuverability	I wish the system is easily maneuverable
368	Data format	I wish the system data format is clear
369	Ability to pull data – queries	I wish the system has the ability to pull data queries
370	Titles should be correct	I wish the data column titles are correct
371	System for help – online or phone	I wish the system has online or phone help
372	Graphing capabilities	I wish the system has graphing capabilities
373	No training	I wish the system does not require training
374	No graphic capabilities trends, budgets vs. actual, communication info to audience	I wish the system has graphing capabilities to compare budgets vs. actual and communicate the information to the audience

375	Cumbersome to generate	I wish the system is not cumbersome to generate reports
376	Don't know how to use	I wish the system is easy to use
377	Titles are not accurate	I wish the data column titles are correct
378	Change data before passing on	I wish the system allows me to change the data before I pass it on
379	Training inadequate	I wish the off-site (online) training I have taken is adequate for the system use
380	-Could not understand	I wish I could understand the system training
381	-not usable features demonstrated and hrs.	I wish the system training has shown relevant demonstrations
382	Online and phone support	I wish the system has online and phone support
383	Questions – got to someone in planning department	I wish the system has centralized support
384	work not getting done	I wish the system helps me get my work done
385	Getting user permissions for everything	I wish the system does not ask for permissions for everything
386	Multiple click through access	I wish the system has no multiple click through
387	Regular trouble accessing email	I wish the system has no troubles
388	Receiving permissions	I wish the system received permissions
389	Ideally options to password everything, opposite,	I wish the password options are clear
390	Time log out, security feature	I wish the system would not time out or log out
391	Restriction is an annoyance, philosophical Microsoft control convenience, quick but annoying	I wish the system would not time out or log out
392	Must give correct answers most of the time.	I wish the system gives correct answers most of the time.
393	Must be fast enough	I wish the system is fast enough

394	Must be only complicated enough to make it work. (Similar to KISS)	I wish the system is only complicated enough to make it work. (Similar to KISS)
395	Must be simple enough so that users understand the functionality of the system.	I wish the system is simple enough so that users understand the functionality of the system.
396	Must be able to share results between users to collaborate effectively	I wish the system is able to share results between users to collaborate effectively
397	Must be integrated with other systems.	I wish the system is integrated with other systems.
398	Must have 99% uptime	I wish the system has 99% uptime
399	Must be able to add new data in a fast manner	I wish the system is able to add new data in a fast manner
400	Must be able to fix broken data in a fast manner	I wish the system is able to fix broken data in a fast manner
401	Must be able to find new ways of exploiting data sets.	I wish the system is able to find new ways of exploiting data sets.
402	It should work on the majority off cases/types directly out of the box with no special configurations or customizations. Someone with no experience with the tool (how would they choose a customization) should be able to get it to work immediately on their basic problem.	I wish the system is easy to use without any prior experience
403	The tool, its setup and its buttons should never rely on tool-specific language. Use a community accepted standard (e.g. image, document, save, open, etc).	I wish the system uses community accepted standard language and set up choices

404	Speed is an issue. With the exception of a development tool and hitting "compile" or running a database query, the program should never take enough time to do a task to be noticeable. e.g. if I have to wait a few seconds between hitting button1 and button2, it's broken.	I wish the system processes tasks with speed
405	The user should never, ever need to understand the underlying pipes. e.g. if you are building a database query gui, the user shouldn't need to know sql syntax to use it.	I wish the system's user interface is simple enough so the user does need to understand the background language/syntax
406	If there are multiple choices for a tool (many versions), a clear grid laying out which choice works best for which setup is essential.	I wish the system has multiple versions/setups for the users to choose
407	Hire a tech-writer. Standardize word choice. if you call something a FooMonster once, don't later refer to it as FooM, or Foo, or Monster.	I wish the system's help is standard and professional
408	Pay attention to the look and feel. Flashing graphics are an annoyance. Black text on a white screen are bad for most people with visual disabilities (blue on yellow is best!). Don't clutter.	I wish the system is visually appealing (without any flashing graphics or black and white text) for all people including people with disabilities
409	Does the tool actually do what it claims to do (and therefore what I need it to do)?	I wish the system does what it claims to do
410	Ease of use, can sort on album name, artist, song	I wish the system has ease of use and can sort on album name, artist, song
411	Search feature in apple store – can type in anything, album, song, artist – and it will find all	I wish the system has search feature in apple store – can type in anything, album, song, artist – and it will find all

412	Can't upload songs from multiple computers to one iPod device	I wish the system allows to upload songs from multiple computers to one iPod device
413	Updates from Apple are too frequent and too large	I wish the system updates are not too frequent and smaller in size
414	Updates from Apple are too frequent and too large	I wish the system updates are not too frequent and smaller in size
415	Purchased songs from itunes can't be shared with others (licensing issues)	I wish the system allows me to share my songs without any licensing issues

Appendix-C: List of Common Form Values

#	Common Form Values
1	I wish the data presentation is better organized
2	I wish the external access is linked to organizational roles
3	I wish the search and navigation features of the system allow me to find the information faster
4	I wish the system allows for easy updates and editing
5	I wish the system features are designed from scratch, not patched something together
6	I wish the system allows external access for research purposes
7	I wish the system allows features to be managed administratively
8	I wish the system allows flexibility in accomplishing tasks
9	I wish the system allows for better search options
10	I wish the system allows for e-commerce
11	I wish the system allows for use of multiple accessories
12	I wish the system allows navigation and purchase of items easier and quicker
13	I wish the system allows quick information access
14	I wish the system allows remote access
15	I wish the system avoids delays
16	I wish the system can assign functionality easily and conveniently
17	I wish the system can be used without interacting with the developer's or user's forum
18	I wish the system can differentiate between trusted and untrusted login attempts
19	I wish the system can retrieve historical data
20	I wish the system consists of all components
21	I wish the system could recognize the trusted user devices
22	I wish the system customizable interface
23	I wish the system does not require login
24	I wish the system displays accurate product information
25	I wish the system displays the process visually
26	I wish the system documentation is easily available
27	I wish the system documentation is well written
28	I wish the system does not collect redundant data
29	I wish the system does not confuse the users
30	I wish the system does not display corrupted data
31	I wish the system does not freeze during processing
32	I wish the system does not give cryptic error messages
33	I wish the system does not have longer periods of pause
34	I wish the system does not have too many different platforms

35	I wish the system does not overwrite base files only after notifying and asking the user
36	I wish the system does not redirect me to some other vendors
37	I wish the system enables better data transfers
38	I wish the system enables data integration
39	I wish the system enables data integration
40	I wish the system enhancements are better communicated
41	I wish the system ensure privacy with multiple users' interaction
42	I wish the system ensures the data integrity during data transfer
43	I wish the system ensures the process fairness
44	I wish the system executes commands accurately
45	I wish the system generated output/results are easily manipulated and interpreted.
46	I wish the system generates automatic alerts
47	I wish the system has archival functionality
48	I wish the system has better accessibility
49	I wish the system has better appearance
50	I wish the system has better collaboration with easy to use tools to help coordination efforts
51	I wish the system has better explanatory features
52	I wish the system has better features
53	I wish the system has better functionality
54	I wish the system has better interoperability
55	I wish the system has better navigation features
56	I wish the system has better version control
57	I wish the system has built in encryption
58	I wish the system has built-in automated internal controls
59	I wish the system has built-in escalation if things go wrong
60	I wish the system has clarity
61	I wish the system has consistent look across all components
62	I wish the system has enhanced reporting capabilities
63	I wish the system has esthetic features
64	I wish the system has faster data processing
65	I wish the system has faster processing of multiple protocols
66	I wish the system has good and flexible security
67	I wish the system has good demonstrations
68	I wish the system has good display
69	I wish the system has good speech recognition
70	I wish the system has identify theft protection
71	I wish the system has instant user support
72	I wish the system has membership interaction
73	I wish the system has minimizes interruptions
74	I wish the system has multi functional currency features
75	I wish the system has no lock-outs or automated session time-outs

76	I wish the system has no major configurations or customizations
77	I wish the system has no maximum user limitation.
78	I wish the system has password recovery
79	I wish the system has security and privacy
80	I wish the system has security questions/images
81	I wish the system has self-to-do model without any professional assistance
82	I wish the system has the ability to download without any interruption
83	I wish the system has the ability to export and generate adequate reports
84	I wish the system has the ability to post closing transactions
85	I wish the system has unlimited storage/archive
86	I wish the system helps make data available without interruption
87	I wish the system helps manipulate data
88	I wish the system helps me connect with international contacts via email, chat and cell phone for low cost
89	I wish the system helps organize online and offline data
90	I wish the system helps organize sensitive data
91	I wish the system helps protect data with multi-layer security
92	I wish the system helps with better personal organization
93	I wish the system improves the productivity
94	I wish the system increases performance of the processes
95	I wish the system installation is automatic to launch at least the basic version/view
96	I wish the system instructions are easy to understand
97	I wish the system interacts well with mobile devices
98	I wish the system interface is understandable
99	I wish the system interprets my intentions correctly
100	I wish the system is adaptable
101	I wish the system is available without any interruption
102	I wish the system is compatible with other and new systems
103	I wish the system is contemporary
104	I wish the system is convenient to use
105	I wish the system is easy to learn
106	I wish the system is easy to learn
107	I wish the system is easy to navigate
108	I wish the system is easy to operate
109	I wish the system is easy to update
110	I wish the system is efficient in performing tasks and producing reports
111	I wish the system is indispensable
112	I wish the system is inexpensive to manage
113	I wish the system is more efficient
114	I wish the system is not too restrictive
115	I wish the system is simple in appearance
116	I wish the system is smart with built in intelligence

117	I wish the system is standardized across functionalities
118	I wish the system is supported by a consolidated database
119	I wish the system is supported by a real-time database
120	I wish the system is user friendly
121	I wish the system is web based
122	I wish the system limit staff visibility
123	I wish the system manages the associated risks
124	I wish the system matches intended goals with expected outcomes
125	I wish the system minimizes unauthorized access
126	I wish the system monitors product delivery
127	I wish the system operates with fewer number of steps
128	I wish the system organization is intuitive
129	I wish the system owner dictate the access administration levels
130	I wish the system prevents the identity thefts
131	I wish the system prevents unnecessary lock outs
132	I wish the system processes real time transactions and operates smoothly
133	I wish the system promotes collaboration
134	I wish the system protects sensitive data
135	I wish the system provides a safe environment
136	I wish the system provides better security
137	I wish the system provides better security
138	I wish the system provides context specific support
139	I wish the system provides disaster recovery support
140	I wish the system provides geographic location features
141	I wish the system provides good user support
142	I wish the system provides interconnectivity between components
143	I wish the system provides standard multi-language support
144	I wish the system remembers my personal data
145	I wish the system retrieves personal data confidentially
146	I wish the system saves personal data confidentially
147	I wish the system saves time
148	I wish the system searches are semantic based
149	I wish the system sends updated messages and notifications for users
150	I wish the system shows improvement from previous versions
151	I wish the system supports multi platform processing
152	I wish the system survives environmental changes and has durability
153	I wish the system transfers personal data confidentially
154	I wish the system upgrades happen automatically
155	I wish the system user support is easily accessible
156	I wish the system uses colors and combinations well in presentation
157	I wish the system writes information as required

158	I wish the system's features are better organized
159	I wish the system's performance is reliable
160	I wish the system's performance is reliable
161	I wish the training is adequate and appropriate
162	I wish the utility of the system is not poor
163	I wish users can compartmentalize sign in for different parts of the system
164	I with the system processes remain uninterrupted

Appendix-D: List of Usability Objective Clusters and Associated Values

#	Raw Values	Cleaned up Raw Values	Common Form Values	Usability Sub-Objective	Usability Objective Cluster	Cluster #
1	Not too sensitive to environmental changes. Value more durability	I wish the system is not too sensitive to environmental changes and is durable	I wish the system survives environmental changes and has durability	Ensure hardware robustness	Maximize system maintainability	1
2	Also using radio systems and other hardware that appear to be old and out of date	I wish the systems and hardware are not outdated	I wish the system is contemporary	Ensure system are up to date	Maximize system maintainability	1
3	Upgrades should happen (or at least announce themselves) automatically	I wish the system upgrades happen automatically	I wish the system upgrades happen automatically	Maximize automatic system upgrades	Maximize system maintainability	1
4	As far as EMS system is concerned, would want a more user-friendly version, more accurate with schedules, more flexible for users.	I wish the system is user friendly, with better version control and accurate and flexible	I wish the system has better version control	Maximize system version control	Maximize system maintainability	1

5	No user maximum.. unlimited users (less licenses) to prevent purchases of licenses	I wish the system has no maximum user limitation.	I wish the system has no maximum user limitation.	Minimize application licensing restrictions	Maximize system maintainability	1
6	Value cheaper/easier upgrade options	I wish the system has cheaper and easier upgrade options	I wish the system is inexpensive to manage	Minimize the total cost of ownership	Maximize system maintainability	1
7	Adaptability	I wish the system is adaptable	I wish the system is adaptable	Maximize system adaptability	Maximize system integrity	2
8	Sometimes not reliable as item does not reach me always (a buy, not reach)	I wish the delivery of the items ordered is reliable	I wish the system's performance is reliable	Maximize system reliability	Maximize system integrity	2
9	Limit staff visibility	I wish the system limit staff visibility	I wish the system limit staff visibility	Maximize automation of manual tasks	Maximize task efficiency	3
10	Successful completion, efficiency in daily tasks (workforce reduction), real time reports, smoother operation, automatic controls	I wish the system is efficient	I wish the system is efficient in performing tasks and producing reports	Maximize efficiency of system tasks	Maximize task efficiency	3

11	There should be at least 2 ways to accomplish the same thing. This could be menu-based vs. key-based. Or 2 different ways through a menu. People's minds are set up differently. Accommodate them.	I wish the system allows to accomplish the same task in multiple ways to allow different types of users and their learning abilities	I wish the system allows flexibility in accomplishing tasks	Maximize flexibility in task processing	Maximize task efficiency	3
12	eBay is not responsible for any transaction (Easy, but not responsive)	I wish the system is responsive and responsible to transactions	I wish the system has built-in escalation if things go wrong	Ensure exception reports go to management	Enhance system related communications	4
13	Give me what I want and use is not what you want to give me	I wish the system give me what I want and use is not what you want to give me	I wish the system writes information as required	Ensure stakeholders intentions are considered	Enhance system related communications	4
14	New system changes	I wish the system enhancements are better communicated	I wish the system enhancements are better communicated	Increase communication of system enhancements	Enhance system related communications	4
15	Would like for GPS to provide crash feedback, be able to call for help	I wish the system provides crash feedback and calls for help	I wish the system generates automatic alerts	Maximize automatic escalation alerts	Enhance system related communications	4
16	Self-to-do model and not professional assistance	I wish the system has self-to-do model without any professional assistance	I wish the system has self-to-do model without any professional assistance	Minimize user interaction with system developers	Enhance system related communications	4

17	If your tool needs a developer's forum (for setup, not for here's my new neat trick with it), or a user's forum, you've failed in usability.	I wish the system can be used without interacting with the developer's or user's forum	I wish the system can be used without interacting with the developer's or user's forum	Minimize users' interaction with technical personnel	Enhance system related communications	4
18	Connect with people via email, chat email and cell phone – International contacts, low cost	I wish the system helps me connect with international contacts via email, chat and cell phone for low cost	I wish the system helps me connect with international contacts via email, chat and cell phone for low cost	Enhance connectivity at affordable price	Maximize system administration functionality	5
19	Everything laid out – easy to be seen – visual, clear and organized	I wish the system lays out features clearly, visually and organized	I wish the system's features are better organized	Ensure system features are organized	Maximize system administration functionality	5
20	Administration of features	I wish the system has administration features	allows features to be managed administratively	Maximize system administration features	Maximize system administration functionality	5
21	Installation should be completely automated and launch at least the basic version/view.	I wish the system installation is automatic to launch at least the basic version/view	I wish the system installation is automatic to launch at least the basic version/view	Maximize ease of system installation	Maximize system administration functionality	5
22	Accurate execution – sometimes not very dependable	I wish the system executes accurately	I wish the system executes commands accurately	Maximize process execution accuracy	Maximize system reliability	6

23	Successful completion, efficiency in daily tasks (workforce reduction), real time reports, smoother operation, automatic controls	I wish the system processes real time transactions and operates smoothly	I wish the system processes real time transactions and operates smoothly	Maximize reliable real-time processing	Maximize system reliability	6
24	Owner should dictate access administration levels	I wish the system owner dictate the access administration levels	I wish the system owner dictate the access administration levels	Maximize system owners' responsibility for errors	Maximize system reliability	6
25	eBay itself should involve a risk	I wish the system involves some risk	I wish the system manages the associated risks	Minimize application risks	Maximize system reliability	6
26	A user manual must be available for ease of use and to answer questions	I wish a system user manual is available for ease of use and to answer questions	I wish the system documentation is easily available	Ensure easy access to system documentation	Clarify & improve system document ation	7
27	More use of sense/voice and less of keyboard to save time	I wish the system users more of sense/voice and less of keyboard to save time	I wish the system documentation is well written	Improve system documentation	Clarify & improve system document ation	7
28	My problem with that is when certain web pages blocked others got also effected which I use for my work	I wish the system does not block web pages that I use for my work	I wish the external access is linked to organizational roles	Define role-based external access	Maximize system access	8

29	My problem with that is when certain web pages blocked others got also effected which I use for my work	I wish the system does not block web pages that I use for my work	I wish the system allows external access for research purposes	Ensure authorized external access	Maximize system access	8
30	Security and firewall features must be available to prevent increases and hacking	I wish the system security and firewall features must be available to prevent increases and hacking	I wish the system minimizes unauthorized access	Minimize system unauthorized access	Maximize system access	8
31	Value ease of use, user friendly, visually appealing, simplistic.	I wish the system is visually appealing	I wish the system has better features	Enhance application features	Maximize system capability	9
32	Ease of purchase – navigation is simple and quick	I wish the system allows navigation and purchase of an item easier and quicker	I wish the system allows navigation and purchase of items easier and quicker	Enhance e-commerce features	Maximize system capability	9
33	Be able to clarify and understand options	I wish to be able to understand and clarify options	I wish the system has better explanatory features	Enhance explanatory features in the system	Maximize system capability	9
34	911 location giving nearest street plus latitude and longitude (for off road)	I wish the system can give location, latitude and longitude options	I wish the system provides geographic location features	Enhance geographic location features	Maximize system capability	9
35	Language features (Arabic, English)	I wish the system has multiple language support	I wish the system provides standard multi-language support	Enhance standard multi-language support	Maximize system capability	9

36	Long waiting time (i-pod charger reach after 1 month, but prince is very less)	I wish there is no waiting period to receive the product	I wish the system monitors product delivery	Ensure tracking of products	Maximize system capability	9
37	Easily manipulative and interpretable output/results – clear results that can be used effectively.	I wish the system generates output/results that could be easily manipulated and interpreted.	I wish the system generated output/results are easily manipulated and interpreted.	Ensure useful reporting features	Maximize system capability	9
38	Multi functional currency – for international firm	I wish the system has multi functional currency features	I wish the system has multi functional currency features	Maximize global trading features	Maximize system capability	9
39	Verbal interface with good speech recognition	I wish the system has verbal interface with good speech recognition	I wish the system has good speech recognition	Maximize speech recognition capabilities	Maximize system capability	9
40	User must have reporting features to meet needs	I wish the system has reporting features to meet the needs	I wish the system has enhanced reporting capabilities	Maximize system reporting capabilities	Maximize system capability	9
41	See all options and customized for each department so people do not	I wish the system has all options and customized for each department so people do not get confused	I wish the system customizable interface	Enhance customizable interfaces	Maximize standardization of system features	10
42	Cryptic error messages	I wish the system does not give cryptic error messages	I wish the system does not give cryptic error messages	Ensure clarity and conciseness in standard error messages	Maximize standardization of system features	10

43	Updated info should be sent as messages eg. Email alerts to notify users.	I wish the system sends updated messages and notifications for users	I wish the system sends updated messages and notifications for users	Maximize standardized automatic user notification alerts	Maximize standardization of system features	10
44	Different standards for different functionalities	I wish the system did not have different standards for different functionalities	I wish the system is standardized across functionalities	Maximize functional standardization	Maximize standardization of system features	10
45	It should work on the majority off cases/types directly out of the box with no special configurations or customizations. Someone with no experience with the tool (how would they choose a customization) should be able to get it to work immediately on their basic problem.	I wish the system has no major configurations or customizations	I wish the system has no major configurations or customizations	Minimize system configuration or customizations	Maximize standardization of system features	10
46	Ease of password recovery	I wish the system allows to recover passwords easily	I wish the system has password recovery	Ensure automated password retrieval	Maximize productivity	11
47	Improve service and reliability	I wish the system has improved service and reliability	I wish the system's performance is reliable	Increase reliability of system performance	Maximize productivity	11
48	Just worked on making it	I wish the system is more efficient	I wish the system is more efficient	Maximize system efficiency	Maximize productivity	11

	more efficient					
49	Ease of use and clear to save time and increase performance	I wish the system increases performance	I wish the system increases performance of the processes	Maximize system performance	Maximize productivity	11
50	At work our network is limited to certain web pages because my boss thinks it decreases the productivity.	I wish the system allows all web pages to increase my productivity	I wish the system improves the productivity	Maximize the system productivity	Maximize productivity	11
51	Security questions/image	I wish the system has security questions/images	I wish the system has security questions/images	Enhance visualization of system security	Maximize system esthetics	12
52	Clarity/color/brightness	I wish the system has clarity/color/brightness	I wish the system uses colors and combinations well in presentation	Ensure color combinations are visually appealing	Maximize system esthetics	12
53	Large screen	I wish the system has large screen	I wish the system has good display	Ensure good application display	Maximize system esthetics	12
54	Appearance – web page needs to look updated or modern to feel more confident in system. Pictures are comforting.	I wish the appearance of the system is better	I wish the system has better appearance	Ensure good system display	Maximize system esthetics	12

55	Clear process visually – no confusion on how to do the next step	I wish the system displays the process visually without any confusion as to how to do the next step	I wish the system displays the process visually	Ensure visualization of system processes	Maximize system esthetics	12
56	Access – able to understand the interface	I wish the system interface is understandable	I wish the system interface is understandable	Maximize ease of navigation in GUIs	Maximize system esthetics	12
57	Correct interpretation of my intent – I want exactly what I want, nothing more.	I wish the system interprets my intentions correctly	I wish the system interprets my intentions correctly	Maximize Graphic User Interfaces	Maximize system esthetics	12
58	Clarity/color/brightness	I wish the system has clarity/color/brightness	I wish the system has esthetic features	Maximize the esthetic system features	Maximize system esthetics	12
59	Being able to visit sites without any interruptions (pop ups and cookies)	I wish the browser allows me to visit sites without any interruptions	I wish the system has minimizes interruptions	Minimize system down-time	Minimize system interruptions	13
60	The system must not freeze to avoid delays	I wish the system does not freeze	I wish the system does not freeze during processing	Minimize system freezes and crashes	Minimize system interruptions	13
61	Longer periods of pause	I wish the system does not have longer periods of pause	I wish the system does not have longer periods of pause	Minimize system response time	Minimize system interruptions	13

62	Value balance between protecting themselves from liability and be able to maintain functionality while reviewing. Locks out a little too much	I wish the system values functionality and does not lock out too much	I wish the system prevents unnecessary lock outs	Minimize unnecessary system lock outs & time outs	Minimize system interruptions	13
63	Alt route suggestions	I wish the system has alternative route suggestions	I wish the system has better navigation features	Ensure ease of navigation through application	Maximize ease of use	14
64	Value simplified web-page appearance	I wish the web pages are simplified in appearance	I wish the system is simple in appearance	Ensure simplicity of the applications	Maximize ease of use	14
65	Tools (are categorized in a way that takes you there with common sense)	I wish the system tools are categorized in a way that takes you there with common sense	I wish the system organization is intuitive	Ensure system usage is intuitive	Maximize ease of use	14
66	Value ease of use, user friendly, visually appealing, simplistic.	I wish the system is user friendly	I wish the system is user friendly	Ensure the user friendly features	Maximize ease of use	14
67	Ease to use, convenient	I wish the system is easy to use and convenient	I wish the system is convenient to use	Maximize convenience of application use	Maximize ease of use	14
68	Ease to navigate	I wish the system is easy to navigate	I wish the system is easy to navigate	Maximize ease of system navigation	Maximize ease of use	14
69	Ease of operation	I wish the system is easy to operate	I wish the system is easy to operate	Maximize ease of system operability	Maximize ease of use	14

70	Not require prior training / less tedious	I wish the system can be used without any prior training and the system is less tedious	I wish the system is easy to learn	Maximize ease of system use	Maximize ease of use	14
71	Fewer number of clicks	I wish the system has fewer number of clicks	I wish the system operates with fewer number of steps	Minimize number of system operating steps	Maximize ease of use	14
72	Type basic information and get faculty resource/information	I wish the system lets me type basic information and get faculty resource/information	I wish the system searches are semantic based	Ensure semantic based search features	Improve system search capability	15
73	Main menu with many search options	I wish the system has many search options	I wish the system allows for better search options	Maximize efficiency of system searches	Improve system search capability	15
74	Ease of navigation – finding what I need fast and with ease. No difficulties involving not being able to figure systems working process out	I wish the search and navigation features of the system allow me to find the information faster	I wish the search and navigation features of the system allow me to find the information faster	Maximize quick search options	Improve system search capability	15
75	Web base	I wish the system is web based	I wish the system is web based	Ensure web access to the system	Maximize database and system access	16
76	Detailed database large	I wish the system is supported with detailed and large database	I wish the system is supported by a consolidated database	Increase consolidation of databases	Maximize database and system access	16
77	Large buttons when driving mode	I wish the system has large buttons to use when driving	I wish the system has better accessibility	Maximize accessibility	Maximize database and system access	16

78	Live traffic data interface	I wish the system has live traffic data interface	I wish the system is supported by a real-time database	Maximize application support by real-time databases	Maximize database and system access	16
79	Would like to access accounts through smart phone	I wish to access accounts through smart phone	I wish the system interacts well with mobile devices	Maximize interoperability of systems and databases with mobile devices	Maximize database and system access	16
80	Ideally windows should not have tried to copy Apple with Vista	I wish the system should have been design from scratch without copying from other systems	I wish the system features are designed from scratch, not patched something together	Ensure functionality is designed into system	Maximize system integration	17
81	Good security – flexibility needed	I wish the system has good and flexible security	I wish the system has good and flexible security	Maximize flexibility of system components	Maximize system integration	17
82	Mouse be able to click on it,	I wish I could the mouse	I wish the system allows for use of multiple accessories	Maximize hardware compatibility	Maximize system integration	17
83	A well connected system (be able to email to oneself from outside search engines)	I wish the system is well connected (be able to email to oneself from outside research engines)	I wish the system has better interoperability	Maximize system interoperability	Maximize system integration	17
84	Can be synched with other systems and new system	I wish the system can be synched with other and new systems	I wish the system is compatible with other and new systems	Maximize system software compatibility	Maximize system integration	17
85	-Different platforms	I wish the system does not have too many different platforms	I wish the system does not have too many different platforms	Minimize multiple system platforms	Maximize system integration	17

86	Training	I wish there is training for the system	I wish the training is adequate and appropriate	Enhance system training quality	Maximize self-efficacy in training	18
87	The Help Button should launch you to a very specific part of the documentation based on your query. It should never be online docs (who is connected when you need help!)	I wish the system's help should be context specific and should not be generic online documents	I wish the system provides context specific support	Ensure user support is context specific	Maximize self-efficacy in training	18
88	A sample use of the tool should be provided. i.e. provide a set of inputs, and setups so that the user can run the program once without having to know it in order to see it at work and understand how it does things. If there is lots of different functionality, provide one example per functionality type.	I wish the system has the ability to show potential users of the sample use without any complex inputs and set ups	I wish the system has good demonstrations	Implement good demos for user support	Maximize self-efficacy in training	18

89	Help desk or user manual easily accessible	I wish the system has help desk or user manually easily accessible	I wish the system user support is easily accessible	Maximize accessibility of user support	Maximize self-efficacy in training	18
90	Instant support	I wish the system has instant support	I wish the system has instant user support	Maximize real-time user support	Maximize self-efficacy in training	18
91	Easy to user resources – online for help support	I wish system provides online user resources for help support	I wish the system provides good user support	Maximize reliable user support	Maximize self-efficacy in training	18
92	Training – most performed as open	I wish the system has less training	I wish the system is easy to learn	Minimize the training required to use the system	Maximize self-efficacy in training	18
93	History and archive of my past purchases, interests, etc. to make recommendations	I wish the system keeps the history and archive of my past purchases, interests, etc. to make recommendations	I wish the system has archival functionality	Ensure data archival functionality	Improve data organization	19
94	Ability to go back to most recent page	I wish the system has the ability to go back to most recent page	I wish the system can retrieve historical data	Ensure data retrieval feature	Improve data organization	19
95	On/off road options/data	I wish the system has multiple options for data	I wish the system helps organize online and offline data	Increase organization of online and offline data	Improve data organization	19
96	Sometimes you get a good deal	I wish I get a good deal	I wish the system ensures the process fairness	Ensure process fairness	Maximize system efficiency	20
97	Could make do with another but not	I wish the system is indispensable	I wish the system is indispensable	Ensure system is indispensable	Maximize system efficiency	20

98	I would like to make special effort to understand instructions	I wish the system's instructions are easy to understand	I wish the system instructions are easy to understand	Increase understanding of system	Maximize system efficiency	20
99	Clarity – shows menus in clear way - does not use funny terms. Unsure…	I wish the menus in the system have clarity	I wish the system has clarity	Maximize system clarity	Maximize system efficiency	20
100	Utility is poor = data not able to be pulled	I wish the utility of the system is not poor	I wish the utility of the system is not poor	Maximize the utility of the system	Maximize system efficiency	20
101	Windows 7 seems to be an improvement	I wish the system shows improvement from previous versions	I wish the system shows improvement from previous versions	Monitor evolution of system capabilities	Maximize system efficiency	20
102	Back up of data	I wish the system backs up data	I wish the system helps make data available without interruption	Ensure data availability	Maximize disaster recovery	21
103	Hours I can access the information	I wish the system allows me to access my information	I wish the system is available without any interruption	Increase system availability	Maximize disaster recovery	21
104	Not too many pop-ups or stop gap ads that slow down the process when trying to go to a different page or through checking out	I with the system does not have too many pop ups or stop gap ads that slow down the process when trying to go to a different page or through checking out	I with the system processes remain uninterrupted	Maximize business process continuity	Maximize disaster recovery	21
105	For in dash a crash sensor feedback like onstar	I wish the system has a crash sensor for feedback like onstar	I wish the system provides disaster recovery support	Maximize disaster recovery support	Maximize disaster recovery	21

106	Like integrating data from the websites - like having UPS tracking number without having to go to UPS website	I wish the system integrates data from the websites	I wish the system enables data integration	Enhance data integrity	Maximize data quality	22
107	Ability to exchange data with Meditech system	I wish the system has the ability to exchange data with Meditech system	I wish the system enables better data transfers	Ensure ability to execute transfer data quickly	Maximize data quality	22
108	Closing the month AP – software let you go back and make changes to revenue which requires too much work	I wish the system has the ability go back and make changes to revenue which requires too much work	I wish the system allows for easy updates and editing	Increase ease in editing and updating of application data accurately	Maximize data quality	22
109	Speed – how quickly wanted information can be accessed and provided.	I wish the system allows information access quickly	I wish the system allows quick information access	Increase timely application data access	Maximize data quality	22
110	Adequate reports – ability to export	I wish the system has the ability to export and generate adequate reports	I wish the system has the ability to export and generate adequate reports	Maximize interoperability of data manipulation	Maximize data quality	22
111	No form	I wish there are no forms	I wish the system does not collect redundant data	Minimize redundant data collection	Maximize data quality	22
112	Too restrictive	I wish the system is not too restrictive	I wish the system is not too restrictive	Decrease restrictiveness of system	Maximize security & privacy	23

113	Encrypts (whenever visiting Korean sites)	I wish the browser encrypts whenever I visit Korean sites	I wish the system has built in encryption	Maximize automatic data encryption	Maximize security & privacy	23
114	Having the option of saving all passwords along with the master password	I wish the browser has the option of saving all passwords along with the master password	I wish the system transfers personal data confidentially	Maximize confidentiality of data	Maximize security & privacy	23
115	Privacy - Windows multiple users, identify theft	I wish the system has identify theft protection	I wish the system has identify theft protection	Maximize identity theft protection features	Maximize security & privacy	23
116	Securing data with multi level security is important with data – lock out/s at session end is good	I wish the system secures the data with multi level security and automated lock outs and session ends	I wish the system helps protect data with multi-layer security	Maximize multi-layer security	Maximize security & privacy	23
117	Value balance between protecting themselves from liability and be able to maintain functionality while reviewing. Locks out a little too much	I wish the system values functionality and does not lock out too much	I wish the system could recognize the trusted user devices	Maximize recognition of trusted and secure devices	Maximize security & privacy	23
118	On Amazon.com, no need to login (saves time)	I wish the system does not require any login to save time	I wish the system does not require login	Maximize single-sign-on authentication	Maximize security & privacy	23

119	Value balance between protecting themselves from liability and be able to maintain functionality while reviewing. Locks out a little too much	I wish the system values functionality and does not lock out too much	I wish the system can differentiate between trusted and untrusted login attempts	Maximize trust in security in network connections	Maximize security & privacy	23
120	Achievement of goals leads to my expected outcome	I wish the system helps me achieve my goals with expected outcomes	I wish the system matches intended goals with expected outcomes	Ensure system functionality meets requirements	Maximize user requirements elicitation	24
121	Successful completion, efficiency in daily tasks (workforce reduction), real time reports, smoother operation, automatic controls	I wish the system has several features including successful completion, efficiency in daily tasks (workforce reduction), real time reports, smoother operation, automatic controls	I wish the system has built-in automated internal controls	Maximize automated internal controls	Maximize user requirements elicitation	24
122	Collaboration with easy to use tools to help coordination efforts	I wish the system has better collaboration with easy to use tools to help coordination efforts	I wish the system has better collaboration with easy to use tools to help coordination efforts	Maximize collaboration through system use	Maximize user requirements elicitation	24
123	Smart system	I wish the system is smart	I wish the system is smart with built in intelligence	Maximize intelligence in applications	Maximize user requirements elicitation	24

124	Collaboration	I wish the system promotes collaboration	I wish the system promotes collaboration	Maximize user collaboration in systems	Maximize user requirements elicitation	24
125	Membership interaction	I wish the system has membership interaction	I wish the system has membership interaction	Maximize user interaction	Maximize user requirements elicitation	24
126	See all options and customized for each department so people do not	I wish the system has all options and customized for each department so people do not get confused	I wish the system does not confuse the users	Minimize user confusion	Maximize user requirements elicitation	24
127	The process must be simple to avoid stress and training, which is to save time	I wish the system saves time	I wish the system saves time	Proactively design applications	Maximize user requirements elicitation	24

Appendix-E: Case of a Computer Hack

CASE 1

CASE OF A COMPUTER HACK*

THIS CASE study is based on a series of events that occurred over a period of two years at the Stellar University (SU), which is an urban university. SU caters primarily to commuter students and offers a variety of available majors, including engineering, theater, arts, business, and education.

SU is a public educational institution that contains a diverse range of technologies. In general, if it exists in the information systems realm, at least one example of the technology can be located somewhere on campus. Mainframe, AS400, Linux, VAX, Unix, AIX, Windows (versions 3.1 to 2003 inclusive), Apple, RISC boxes, SANs (storage area networks), NASs (network attached storage), and whatever else has been recently developed is functioning in some capacity. The networking infrastructure ranges from a few remaining token ring locations to 10/100/1000 Mbps Ethernet networks, wireless, and even some locations with dial-up lines. A VPN (virtual private network) is in place for some of the systems shared with the medical portion of the university, primarily due to HIPAA (Health Insurance Portability and Accountability Act of 1996) requirements.

In this open and diverse environment, security is maintained at the highest overall level possible. The computer center network connections are protected by a firewall. Cisco routers are configured as "deny all except," thus only opening the required ports for the applications to work. IDS (intrusion detection systems) devices are installed at various locations to monitor network activity and analyze possible incidents. The systems that are located in the computer room are monitored by network and operating system specialists whose only job is the care and feeding of the equipment.

Servers may be set up by any department or individual under the guise of *educational freedom* and to provide a variety of available technologies to students. For this purpose, many systems are administered by personnel who have other primary responsibilities, or do not have adequate time, resources, or training. If the system is not reported as a server to the network group, no firewall or port restrictions are put into place. This creates an open, vulnerable internal network, as it enables a weakly secured system to act as a portal from the outside environment to the more secured part of the internal network.

The corporate culture is as diverse as the computer systems. Some departments work cooperatively, sharing information, workload, standards, and other important criteria freely with peers. Other areas are "towers of power" that prefer no interaction of any kind outside the group. This creates a lack of standards and an emphasis on finger pointing and

*This case was prepared by Sharon Perez under the supervision of Professor Gurpreet Dhillon. The purpose of the case is for class discussion only; it is not intended to demonstrate the effective or ineffective handling of the situation. The case was first published in the *Journal of Information System Security*, Vol. 1, No. 2. Reproduced with permission.

blame assignment instead of an integrated team approach. Some systems have password expirations and tight restrictions (i.e., mainframe) and some have none in place (domain passwords never expire, complex passwords are not enforced, no password histories are maintained, etc.).

COMPUTER SYSTEM

The server in this situation (let's call it server_1) was running Windows NT 4.0 with service pack 5 and Internet Explorer 4. Multiple roles were assigned to this system. It functioned as the Primary Domain Controller (PDC) (no backup domain controllers (BDCs) were installed or running), WINS (Windows Internet Naming Service) server, and primary file and print server for several departments. In addition, several mission-critical applications were installed on the server. There were few contingencies in place if this server crashed, though the server was a critical part of the university functionality. For example, if the PDC was lost, the entire domain of 800+ workstations would have to be recreated since there was no backup copy of the defined domain security (i.e., no BDC).

To complicate matters, a lack of communication and standards caused an additional twist to the naming convention. On paper, the difference between a dash and an underscore is minimal; in the reality of static DNS (domain name system) running on a Unix server, it is huge. The system administrator included an underscore in the system name (i.e., server_1) per his interpretation of the network suggestion. The operating system and applications (including SQL 7.0 with no security patches) were then installed and the server was deemed production.

As an older version of Unix bind was utilized for the primary static DNS server by the networking group, the underscore was unsupported. There were possible modifications and updates that would allow an underscore to be supported, but these were rejected by the networking group. This technical information was not clearly communicated between the two groups. Once the groups realized the inconsistency, it was too late to easily make major changes to the configuration. Lack of cooperation and communication resulted in each faction coming to its own conclusion: the system administrator could not change the server name without reinstallation of SQL (version 7.0 did not allow for name changes) and a reconfiguration of the 800+ systems that were in the domain. The network group would not make a bind configuration change that allowed for underscores, and instead berated the name server_1, indicating it should have been named server-1, as dashes are supported.

This miscommunication led to further complications of the server and domain structure. Neither group would concede, but the system administrator for the domain had to ensure that the mission-critical applications would continue to function. To this end, the server was further configured to also be a WINS server to facilitate NetBIOS name resolution. As there was no negotiation between the groups, and the server name could not be easily changed, this became a quick fix to allow the production functionality to continue. The actual reason for this fix was not clearly communicated between the groups, thus adding to the misunderstandings.

For various reasons, this server was now running WINS, file and print serving, PDC (no BDC in the domain), and mission-critical applications. In addition, the personnel

conflicts resulted in the server being on an unsecured subnet. In other words, there was no firewall. It was wide open to whomever was interested in hacking it. No one group was at fault for this situation; it was the result of a series of circumstances, technical limitations, and a disparate corporate culture.

The server is an IBM Netfinity, which was built in 1999. At the time of its purchase, it was considered top of the line. As with most hardware, over the years it became inadequate for the needs of the users. Upgrades were made to the server, such as adding an external disk drive enclosure for more storage space and memory.

The manufacturer's hardware warranty expired on the server and was not extended. After this occurred, one of the hard drives in the RAID 5 (Redundant Array of Inexpensive Disks) array went bad (defunct). The time and effort required to research and locate a replacement drive was considerable. A decision was finally made to retroactively extend the warranty, and have the drive replaced as a warranty repair. The delay of several days to accomplish this could have been catastrophic. RAID 5 is redundant, as the name suggests, and can tolerate one lost drive while still functioning at a degraded level. If two drives are defunct, the information on the entire array is lost, and must be restored from backups. Backups are accomplished nightly, but there is still the worst-case scenario of losing up to 23.5 hours of updates if a second drive goes bad just before the backup job is submitted.

CHANGES

Several factors changed during this two-year period. A shift in management focus to group roles and responsibilities as well as a departmental reorganization caused several of the towers of power to be restructured. These intentional changes were combined with the financial difficulties of the province and its resulting decrease in contributions to public educational institutions. The university was forced to deal with severe budgetary constraints and cutbacks.

University management had determined that all servers in the department (regardless of operating system) should be located at the computer center. This aligned with the roles and responsibilities of the computer center to provide an appropriate environment for the servers and employ qualified technical personnel to provide operating system support. Other groups (i.e., application development, database administration, client support) were to concentrate on their appropriate roles, which were much different than server administration. The resistance to change was departmentwide, as many people felt that part of their job responsibilities was taken from them.

Moving the servers to a different physical location meant that a different subnet would be used, as subnets are assigned to a building or geographical area. The existing subnet, as it was not located at the computer center, did not have a firewall. That fact, combined with personnel resistance and a discord between the groups, resulted in quite limited cooperation. For this reason (more politically driven than best-practices inspired), the unsecured subnet was relocated to the computer center intact as a temporary situation.

By the same token, the existing system administrators were not very forthcoming about the current state of the systems, and continued to monitor and administer them remotely. This was adverse to the management edict, but allowed to continue. On a very gradual scale, system administration was transferred to the computer center personnel.

Due to lack of previous interaction between the groups, trust had to be earned as the original system administrators were still held accountable by their users. They would be the ones to face the users if or when the system went down, not the server personnel at the computer center.

HISTORY OF THE SYSTEM

The server (server_1) was relocated on an as-is basis, and the accountability for the server was transferred. Minimal system documentation and history were included, and since the new system administrators had not built the systems, reverse engineering was necessary to determine what software was installed and how the hardware and software was configured. Minor modifications were made to the servers, with appropriate permission, to bring them in line with current standards. Some of the changes broke applications temporarily, as it was a learning process for the new administrator.

For instance, Windows NT 4.0 service pack 6a was not originally applied. This service pack had several patches to eliminate huge security holes that were inherent in NT 4.0. As it was a tenuous working relationship between the groups, all proposed changes had to be reviewed and approved so trust could be established. Each scheduled maintenance window provided its own challenge, as the system was considered by most of the technicians involved to be temperamental.

Simple modifications were made with approval, which did not cause a system outage. These changes were designed to decrease the intrinsic vulnerability of the server. The changes were not implemented previously, as the original system administrator had considerably more work to do than one person could handle. His priority was to fire-fight and keep everything running. Items such as IIS were installed, and services like FTP, WWW, and DHCP were set to "automatic" and "started." These were removed or disabled since they were not being utilized; they only wasted resources and created additional security challenges.

The first off-hours maintenance attempt was quite disastrous. Windows NT 4.0 service pack 6a would not apply (error message of "could not find setup.log file in repair directory"), and had to be aborted. Subsequent operating system–critical updates would not apply for the same reason. SQL 7.0 was also behind on maintenance patches, and the installation of SQL 7.0 service pack 4 was flawless until it hit 57 percent. At that point it would not continue because there was "not enough room to install," and it would not uninstall at that point either. The critical application that used SQL would not launch when signed on locally to the server as an administrator, and had an error. The server was restarted, and was available to the users the next day, though the status of the application was still in question. According to the users, however, the application worked fine the next morning, even though it could not be opened locally on the server.

Research was accomplished to determine how to correct these error messages. Microsoft knowledge-base article 175960 had a suggested corrective action for the "could not find setup.log file" error. Another maintenance window was scheduled and service pack 6a was finally applied to the server. But the version of Internet Explorer (IE) then reverted back to IE version 2.0 and the server forgot it had more than one processor. Further research and off-hours attempts finally allowed all service packs and security patches

to be applied. The single processor problem was corrected via Microsoft knowledge-base article 168132. The IE rollback was corrected by reapplying the 6a service pack.

OTHER ISSUES

To complicate matters further, the provincial government had a serious financial crisis. Budgets were severely cut, and for the first time in recent memory, many state employees were laid off. This reduction of staff power caused numerous departments to eliminate their information systems (IS) support personnel and rely on the university technical infrastructure that was already in place. This further strained the departments that had the roles and responsibilities of the support areas, as they had decreased their staff power also. This resulted in frustration, heavy workloads, and a change in procedures for many departments.

One of the suggestions for an improved operating environment was to replace the current temperamental system (server_1) with new hardware that had an active hardware warranty and ran a current server operating system. This avenue initially met with a considerable number of obstacles, including the fact that the original system administrators were unfamiliar with the new version of the operating system, questions as to whether legacy programs were compatible with the new operating system, and the complication of replacing a temperamental system that was functioning in numerous critical roles.

A joint decision was made between the groups to replace the legacy hardware and restructure the environment in a more stable fashion. Several replacement servers were agreed upon, and a best practices approach was determined. The hardware was then purchased, received, and installed in a rack in the computer center. At that point, lack of staff power, new priorities, resistance to change, and reluctance to modify what currently functioned caused a delay of several months. The project's scope also grew, as the system replacements became linked to a migration to the university active directory (AD) forest.

HACK DISCOVERED

On a Monday morning in February, the system administrator was logged onto the server with a domain administrator account via a remote control product. He noticed a new folder on the desktop, and called the operating system administrator at the computer center. Upon signing on locally with a unique domain administrator-level user ID (i.e., ABJones) and password, there were several suspicious activities that occurred. Multiple DOS windows popped up in succession, the suspect folder was recreated, and the processor usage spiked higher than normal. The new folder was named identically to the one that was just deleted by the other system administrator during his remote session.

As server_1 was previously set up to audit and log specific events (per the article "Level One Benchmark; Windows 2000 Operating System v1.1.7," located at www.cisecurity.org), the Windows event log was helpful in determining the cause of the activities. Several entries for "privileged use" of the user ID that was currently logged on as a domain administrator (ABJones) were listed in the security logs. During the few minutes that the server was being

examined, no security settings were knowingly modified. These circumstances raised further questions, as the more in-depth the system was examined, the more unusual events were encountered.

A user ID of "Ken" was created sometime during the prior weekend, and granted administrative rights. No server maintenance (hardware or software) was scheduled, and none of the system administrators had remotely accessed the server during that time. Event logs indicated that Ken had accessed the server via the TAPI2 service, which was not a commonly used service at the university. The user ID was not formatted in the standard fashion (i.e., first initial, middle initial, first six characters of the last name), and was therefore even more suspect.

Antivirus definitions and the antivirus scan engine on the system were current; however, the process to examine open files was disabled (Symantec refers to this service as *file system realtime protection*). The assumption was that this may have been the first action a hacker took so that the antivirus product did not interfere with the malware application installation. All of these circumstances added up to one immediate conclusion: that the system had most likely been compromised.

IMMEDIATE RESPONSE

Both system administrators had previously read extensively on hacks, security, reactions to compromises, best practices, and much of the other volumes of technical information available. This, however, did not change the initial reaction of panic, anger, and dread. E-mail is too slow to resolve critical issues such as these. The system administrators discussed the situation via phone and came to the following conclusions: disconnect the system from the network to prevent the spread of a possible compromise, notify the security team at the university, and further review the system to determine the scope and severity of the incident.

Each administrator researched the situation and examined the chain of events. It was finally determined that a Trojan was installed on server_1 that exploited the buffer overrun vulnerability that was fixed by Windows critical update MS04-007. This vulnerability was created by Microsoft patch MS03-0041-823182-RPC-Activex, which corrected the Blaster vulnerability. Once the compromise was confirmed, a broader range of personnel were notified, including networking technicians, managers, and technical individuals subscribed to a university security list-serve. A maintenance window had been previously approved to apply the new Microsoft patches to this and several other servers on Thursday, in three days.

FURTHER RESEARCH AND ADDITIONAL SYMPTOMS

Continued examination of the system event logs indicated that a password crack program was executed on the previous Saturday evening using TAPI2 and a valid user ID on the system. Since this server was a domain controller, all other Windows servers were examined. Two additional servers were found to be compromised: one was

a member server in a workgroup, and one was a domain controller for a Windows NT 4.0 domain that had a trust relationship with the hacked domain.

Upon closer examination, several additional changes were noted on the server:

- A scheduled task (At1.job) was created. This task seemed to be set to delete itself once it ran (it was set to run "one time only" and to "Delete the task if it is not scheduled to run again") to remove the hack traces. The job content was one line of code: run cmd /c nc.exe –l –p 20000 –e cmd.exe.
- A new directory was created on the system (c:\winnt\system32\asy).
- When any administrator logged onto the system locally, DOS windows flashed momentarily while the Trojan executed the commands regedit.exe and hiderun.exe.
- Services called Gopher and Web were started; normally these configured as disabled or manual.

Extensive examination of client computer systems within the domain indicated that the attack could have been relayed through another compromised machine at the university. A client system that was located in another area of the campus had the TAPI2 service compromised. The user of this particular system had set the user account password to be the same as the user account ID (i.e., user ID of jksmith has a password of jksmith). This was most likely the weak link that was exploited to gain access to the server.

The DameWare Trojan program DNTUS26 was eventually located on server_1. DameWare provides useful tools for network and system administrators. However, they admit, "With the increased popularity of Internet access, more and more computer systems are being connected to the Internet with little or no system security. Most commonly the computer's owner fails to create a password for the Administrator's account. This makes it very easy for novice hackers ('script kiddies') to gain unauthorized access to a machine. DameWare Development products have become attractive tools to these so-called 'script kiddies' because the software simplifies remote access to machines where the Username & Password are already known. . . . Please understand that the DNTU and/or DMRC Client Agent Services cannot be installed on a computer unless the person installing the software has already gained Administrative access privileges to the machine" (www.dameware.com/support/kb/article.asp? ID=DW100005). There are several Web sites that discuss this Trojan, and offer methods of removing it (two examples are www.net-integration.net/zeroscripts/dntus26.html and www.st-andrews.ac.uk/lis/help/virus/dec20.html).

The overall symptoms of the hack were consistent with the BAT/mumu.worm.c virus (http://vil.nai.com/vil/content/print100530.htm). Netcat (nc.exe) was an active process, which may have been used to open a backdoor and gain access to the system. An ftp server was installed and configured to listen for connections on random ports over 1024. A directory was created on server_1 (c:\winnt\system32\inetsrv\data) and several files were created and placed there. The files in this directory contained information such as user names, passwords, group names, and computer browse lists from other network machines that could be seen from that server. The assumption was that this information was collected for eventual transmission to the hacker(s) to gain additional knowledge of the network environment. Additionally, a key was added to the registry that would reinstall the malware if it was located and removed by a system administrator.

ADDITIONAL VULNERABLE SYSTEMS

The compromise of server_1 was a major security breach at the university. There are approximately 20 member servers and 800 client workstations in that particular domain. Since the primary domain controller was hacked and all of the domain security information was amassed in a hacker-created directory, it was assumed that the entire domain had been compromised. Once the domain administrator account was known, the hacker had full control of all systems within that domain. By default, the domain administrators group was placed into the local administrator group on all client workstations. This is Microsoft's default action and is accomplished for valid security reasons, such as a user leaving the company and not disclosing his or her password to the system. A domain administrator can, for example, access all of the information on that system and retrieve it for business continuity purposes.

In addition, since there was an explicit two-way trust relationship between this domain and another, the PDC in the second domain was also compromised. Security files were found on this second system in similar locations and containing similar types of information. Again, with the domain controller compromised, the two member servers and 100+ workstations that are a part of that domain were also suspect.

IMMEDIATE COUNTERATTACK ACTIONS TAKEN

Before server_1 was reconnected to the network, several actions had to be taken immediately to ensure that the system would not cause any additional security-related problems. The initial task was to clean the servers so that they could be brought back up. System administrators removed all of the malware that had been identified. A list of required ports was compiled to facilitate the firewall configuration by the networking group.

As indicated earlier, there were no password restrictions applied at the domain level, nor any password expiration time period established [group policy objects (GPOs) were not used to set this either, as it is a Windows NT 4.0 domain and GPOs cannot be used on an NT domain]. Many of the users had the same password that was given to them when their account was created! A password policy was enabled (minimum password length of six, maintain history for five passwords, and a one-hour account lockout after five invalid sign-on attempts) and all user IDs were set to "user must change password at next logon." This had to be done manually (open the properties of each user ID and click the appropriate selections, and then click okay) as there were no login scripts, policies, or other means to globally apply the change.

These processes had to be accomplished on each infected system and on each of the compromised domains. The process, however, still left the system administrators uncomfortable as there was insufficient experience in forensics to ensure that all the remnants of the attack were removed. For this reason, an external vendor with the appropriate experience was contracted and requested to certify that the systems were completely cleaned. A computer forensic expert was brought in to accomplish this task and to ensure the return of the systems to full functionality. The vendor developed a series of steps to disable the Trojan and remove the infected files. The procedure was accomplished on the infected servers, as well as about 12 client workstations in the associated domains.

LONG-TERM COUNTERATTACK ACTIONS TAKEN

Once the immediate issues were corrected and the systems were brought back on line, there still remained the postmortem examination to determine what went wrong and why. In this instance, the postmortem was handled informally, and consisted of a summary write-up (for management) and an analysis of how to more effectively block against this type of attack in the future (for system administrators).

Several steps were taken to modify the standard server configurations in an attempt to avoid the same type of compromise in the future. First, the configuration for the open source monitoring tool (Big Brother, http://bb4.com) that is used to report the system status was modified. Most incidents that were reviewed during the research phase of the hack began with a hacker disabling the antivirus product once he or she has gained access to the server. For this reason, the Symantec process that is responsible for real-time file protection was added to the list of services that were monitored. This change would cause system administrators to be paged or e-mailed if the service was stopped, regardless of the reason. It would not prevent intrusion, but would be an early notification tool that something may be amiss.

The temporary password policy changes were made permanent. A university policy change of this magnitude requires approval from several areas within the university. With the recent glaring example of what happened when passwords were not restricted, the policy was approved rather quickly. In addition, the domain accounts are being further reviewed by security personnel to eliminate invalid accounts. Some users have been found with two or three IDs, thus increasing the number of "valid" IDs that can be used as means of attack. This would especially be true if the ID still had its original password.

One of the suggestions from http://vil.nai.com/vil/content/print100530.htm was to delete the administrative shares that are automatically created on each server. The shares are recreated after each system restart, but a batch file can be scripted to disable them upon boot each time. The site suggests:

> *Such worms often rely on the presence of default, administrative shares. It is a good idea to remove the administrative shares (C$, IPC$, ADMIN$) on all systems to prevent such spreading. A simple batch file containing the following commands may be of help, especially when run from a logon script, or placed in the startup folder.*

- net share c$ /delete
- net share d$ /delete
- net share ipc$ /delete
- net share admin$ /delete

Each server is currently configured with a batch file that runs on startup. The batch file gathers system information and places it in a text file on the hard drive, which is backed up nightly. The deletions for the net shares could be tailored to each server and placed in that batch file with minimal effort. This suggestion is still being reviewed by the system administrators.

SUMMARY

This particular incident was an eye-opener for all involved. It was a shock to see how quickly, easily, and stealthily the systems were taken over. The tools that were utilized were all readily available on the Internet. The fact that the password policy was inadequate was already known, though the ramifications of such a decision were not fully explored. It was originally deemed easier to set no password policy than to educate the users, though that opinion drastically changed over the course of a few days.

The financial cost of this compromise has not been calculated, but it would be quite interesting to try to do so: lost time due to the servers being down, vendor contract fees, overtime for technicians (actually, it is compensation time, but it does affect how much additional time the technicians will be out of the office), delays in previously scheduled activities, meetings to determine notification, and discussion of actions to be taken.

Computer forensics, in this case, was used to explore and document what the hacker had done, but not to track down who had gotten into the system. There was not enough knowledge on the system administrators' or contractor's part to begin to track down the culprit. This case was more one of "Get it back up and running quickly and securely" than it was to prosecute the hacker. More surprising, there is a general knowledge of what type of information the servers held, but no concrete idea of what (if anything) was compromised. The details of what was actually compromised may not be apparent until some time in the future.

List of References

Adams, A. and A. M. Sasse (1999). "Users Are Not The Enemy." Communications of ACM **42**(12): 41-46.

Agarwal, R. and V. Venkatesh (2002). "Assessing a firm's Web presence: A heuristic evaluation procedure for the measurement of usability." Information Systems Research **13**(2): 168-186.

Angelou, G. N. and A. A. Economides (2008). "A Decision Analysis Framework for Prioritizing a Portfolio of ICT Infrastructure Projects." IEEE TRANSACTIONS ON ENGINEERING MANAGEMENT **55**(3): 479-495.

Avizienis, A., J.-C. Laprie, et al. (2004). "Basic Concepts and Taxonomy of Dependable and Secure Computing." IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, **1**(1): 11-33.

Backhouse, J. and G. Dhillon (1996). "Structures of responsibility and security of information systems." European Journal of Information Systems **5**(1): 2-9.

Bail, W. G. (2006). "Requirements Management for Dependable Software Systems." Advances In Computers.

Bakke, S., R. Faley, et al. (2005). The Impact of Privacy Concerns on the Use of Information Technologies: A preliminary Conceptual Model. Eleventh Americas Conference on Information Systems, Omaha, NE, USA.

Baskerville, R. (1993). "Information Systems Security Design Methods: Implications for Information Systems Development." ACM Computing Surveys **25**(4): 375-414.

Baskerville, R. and M. T. Siponen (2002). "An Information Security Meta-policy for Emergent Organizations." Logistic Information Management **15**(5/6): 14 pages.

Boland, R. (1978). "The process and product of system design." Management Science **28**(9): 887-898.

Catton Jr., W. R. (1952). "A Theory of Value." American Sociological Review **24**(3): 310-317.

Cavalli, E., A. Mattasoglio, et al. (2004). "Information security concepts and practices: the case of a provincial multi-specialty hospital." International Journal of Medical Informatics **73**: 297-303.

Cranor, L. F. and S. Garfinkel (2005). Security and usability : designing secure systems that people can use. Beijing Sebastopol, CA, O'Reilly.

Darke, P. and G. Shanks (1997). "User Viewpoint Modelling: Understanding and Representing User Viewpoints During Requirements Definition." Information Systems Journal **7**(3).

Davenport, T. H. (2009). "Make Better Decisions." Harvard Business Review.

Davenport, T. H., M. Hammer, et al. (1989). "How Executives Can Shape Their Company's Information Systems." Harvard Business Review: 130-134.

Debrabander, B. and A. Edstrom (1977). "Successful Informatino System Development Projects." Management Science **24**(2): 191-199.

DeWitt, A. J. and J. Kuljis (2006). Aligning Usability and Security: A Usability Study of Polaris. Symposium On Usable Privacy and Security (SOUPS), Pittsburgh, PA, USA.

Dhillon, G. (1995). Interpreting the management of information system security. London School of Economics and Political Science. London, University of London.

Dhillon, G. (1997). Managing information system security. London, Macmillan.

Dhillon, G. (2004). "Dimensions of Power and IS implementation." Information and Management **41**(5).

Dhillon, G. (2007). Principles of Information Systems Security, John Wiley & Sons.

Dhillon, G. and J. Backhouse (2001). "Current directions in IS security research: toward socio-organizational perspectives." Information Systems Journal **11**(2).

Dhillon, G. and G. Torkzadeh (2006). "Value-focused assessment of information systems security in organizations." Information Systems Journal **16**: 293-314.

DiAngelo, M. F. and C. J. Petrun (1995). "Collecting product-based usability requirements." IBM Systems Journal **34**(1).

Dzida, W. (1996). "International Usability Standards." ACM Computing Surveys **28**(1): 3.

Eisenhardt, K. M. (1989). Building theories from case study research. Academy of Management Review. **4:** 532-550.

Eloff, J. and M. Eloff (2003). Information Security Management - A New Paradigm. Proceedings of SAICSIT.

Flechais, I., A. M. Sasse, et al. (2003). Bringing Security Home: A process for developing secure and usable systems. New Security Paradigms Workshop (NSPW 2003), Ascona, Switzerland, ACM.

Folmer, E., J. v. Gurp, et al. (2003). "A Framework for capturing the relationship between usability and software architecture " Software Process: Improvement and Practice Volume 8, Issue 2. Pages 67-87. June 2003 **8**(2): 21.

Furnell, S. M., A. Jusoh, et al. (2005). "The challenges of understanding and using security: A survey of end-users." Computers & Security **25**: 27-35.

George, J. F., D. Batra, et al. (2004). Object-oriented systems analysis and design. Upper Saddle River, N.J., Pearson Prentice Hall.

Gliner, J. A. and G. A. Morgan (2000). Research Methods in Applied Settings: An Integrated Approach to Design and Analysis, Psychology Press.

Gunson, N., D. Marshall, et al. (2011). "User perceptions of security and usability of single-factor and two-factor authentication in automated telephone banking." Computers & Security **30**: 208-220.

Harris, M. A. (2010). THE SHAPING OF MANAGERS' SECURITY OBJECTIVES THROUGH INFORMATION SECURITY AWARENESS TRAINING. Information Systems. Richmond, VA, Virginia Commonwealth University. **Ph.D.**

Harrison, D. (2002). "Security issues for systems used for collecting, storing and interpreting human biological data." Journal of Commercial Biotechnology **8**(4): 304-314.

Henderson, J. C. and J. M. West Jr. (1979). "Planning for MIS: A Decision-Oriented Approach." MIS Quarterly: 45-58.

Hoffman, D., E. Grivel, et al. (2005). "Designing software architectures to facilitate accessible Web applications." IBM Systems Journal **44**(3): 467-483.

Honeyman, P., G. A. Schwartz, et al. (2007). Interdependence of Reliability and Security. 6th Workshop on Economics of Information Security (WEIS).

ISO (1998). Ergonomic requirements for office work with visual display terminals (VDTs) -- Part 11: Guidance on usability. **9241-11**.

ISO/IEC (2005). Information technology -- Security techniques -- Code of practice for information security management, ISO/IEC.

Ives, B., S. Hamilton, et al. (1980). "A Framework for Research in Computer-Based Management Information Systems quick view." Management Science **26**(9): 910-934.

Johnson, M. E. and N. D. Willey (2011). "Usability Failures and Healthcare Data Hemorrhages." IEEE SECURITY & PRIVACY: 8.

Johnston, J., J. H. P. Eloff, et al. (2003). "Security and human computer interfaces." Computers & Security **22**(8): 675-684.

JTC1/SC7, I. I. (2010). Study Group Report on System Integration. Canada, ISO/IEC JTC1/SC7. **2010-04-19**.

Kankanhalli, A., H.-H. Teo, et al. (2003). "An integrative study of information systems security effectiveness." International Journal of Information Management **23**: 139-154.

Karat, J. and C. M. Karat (2003). "The evolution of user-centered focus in the human-computer interaction field." IBM Systems Journal **42**(4): 532-541.

Karlsson, I. C. M. (2000). A holistic approach to usability. Ved Inngangen til Cyberspace – ergonomisk tenkning inn i et nytt årtusen Knut Inge Fostervold og Tor Endestad (Red).

Keeney, R. (1992). Value-focused Thinking: A path to creative decisionmaking. Cambridge, MA, Harvard University Press.

Keeney, R. (1994). "Creativity in decision making with value-focused thinking." Sloan Management Review, 35(4), 33. **35**(4).

Keeney, R. (1996). "Value focused thinking: identifying decision opportunities and creating alternatives." European Journal of Operational Research **92**(13): 537.

Kekre, S., M. S. Krishnan, et al. (1995). "Drivers of Customer Satisfaction for Software Products: Implications for Design and Service Support." Management Science **41**(9): 1456-1470.

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:** 67-94.

Krauss, F. S. H. (2003). "Methodology for remote usability activities: A case study." IBM Systems Journal **42**(4): 582-593.

Lane, V. P. (1985). Security of computer based information systems. Basingstoke, Macmillan.

Larman, C. (2005). Applying UML and patterns : an introduction to object-oriented analysis and design and iterative development. Upper Saddle River, N.J., Prentice Hall PTR.

Leech, J. (2003). "Improving security behavior." Computers & Security **22**(8).

Liimatainen, S. (2005). Usability of Decentralized Authorization Systems – A Comparative Study. 38th Hawaii International Conference on System Sciences, Hawaii, IEEE.

Ma, Q. and M. J. Pearson (2005). "ISO 17799: “BEST PRACTICES” IN INFORMATION SECURITY MANAGEMENT?" Communications of the Association for Information Systems **15**.

Melone, N. P. (1990). "A Theoretical Assessment of the User-Satisfaction Construct in Information Systems Research." Management Science **36**(1): 76-91.

Mishra, S. (2008). DEFINING VALUE BASED INFORMATION SECURITY GOVERNANCE OBJECTIVES. Information Systems. Richmond, VA, Virginia Commonwealth University. **Ph.D.**

Mishra, S. and G. Dhillon (2006). Information systems security governance research: a behavioral perspective. . 1st Annual Symposium on Information Assurance, Academic Track of 9th Annual NYS Cyber Security Conference, , New York, USA.

NIST, N. I. o. S. a. T. (2009). Information Security. Gaithersburg, MD, National Institute of Standards and Technology. **800-53**.

Oltsik, J. (2009). "Protecting Confidential Data Revisited." Enterprise Strategy Group: 49.

Palmer, J. W. (2002). "Web site usability, design, and performance metrics." Information Systems Research **13**(2): 151-167.

Paulheim, H., S. Doweling, et al. (2009). Improving Usability of Integrated Emergency Response Systems: The SoKNOS Approach. 39. Jahrestagung der Gesellschaft fur Informatik e.V. (GI) - Informatik 2009, LNI.

Perez, S. (2005). "Case Study: The Case of a Computer Hack." Journal of Information System Security **1**(2): 10.

Pfleeger, C. P. (1997). "The Fundamentals of Information Security." IEEE SOFTWARE: 15-17.

Power, D. J. (1983). "The Impact of Information Management on the Organization: Two Scenarios." MIS Quarterly **7**(3): 13-20.

Preston, D. S. and D. Chen (2008). "Examining the Antecedents and Consequences of CIO Strategic Decision-Making Authority: An Empirical Study." Decision Sciences **39**(4): 605-642.

PriceWaterhouseCoopers (2011). "Global State of Information Security Survey."

PriceWaterhouseCoopers (2012). Rethinking risk management for new market realities. Risk in Review, PwC**:** 19.

Ratha, N. K., J. H. Connell, et al. (2001). "Enhancing security and privacy in boimetrics-based authentication systems." IBM Systems Journal **40**(3): 614-634.

Rose, J. M., A. M. Rose, et al. (2004). "The Evaluation of Risky Information Technology Investment Decisions." Journal of Information Systems **18**(1): 53-66.

Ryan, S. D. and B. Bordloi (1997). "Evaluating security threats in mainframe and client/server environments." Information & Management **32**: 173-146.

Saaty, T. L. (1980). The Analytic Hierarchy Process B2 - The Analytic Hierarchy Process. New York, McGraw-Hill.

Saaty, T. L. (1990). "How to make a decision: The Analytic Hierarchy Process." European Journal of Operational Research **48**: 9-26.

Saaty, T. L. (2001). The Analytic Network Process: Decision Making With Dependence and Feedback, Rws Pubns;.

Saint-Germain, R. (2005). "Information Security Management Best Practice Based on ISO/IEC 17799." The Information Management Journal: 60-66.

Saltzer, J. H. and M. D. Schroeder (1975). "The Protection of Information in Computer Systems." Proceedings of the IEEE **63**(9): 1278-1308.

Schoemaker, P. J. H. and E. J. Russo (1993). "A Pyramiid of Decision Approaches." California Management Review: 23.

Schultz, E. E., R. W. Proctor, et al. (2001). "Usability and Security An Appraisal of Usability Issues in Information Security Methods." Computers & Security **20**(7): 620-634.

Seffah, A. and E. Metzker (2004). "TheOBSTACLES and MYTHS of USABILITY and SOFTWARE ENGINEERING." Communications of the ACM **47**(12): 7.

Segev, A. and J. Porra (1998). "Internet Security and the Case of Bank of America." Communications of the ACM **41**(10): 81-87.

Sharda, R., S. H. Barr, et al. (1988). "Decision Support System Effectiveness: A Review and an Empirical Test." Management Science **34**(2).

Smith, J. and J. Frisby (2004). "A Five-Step Plan for Comprehensive Information Security and Privacy." Bank Accounting & Finance **17**(4): 31-37.

Straub, D. (1990). "Effective IS Security." Information Systems Research **1**(3): 255-276.

Strong, D. M. and O. Volkoff (2010). "UNDERSTANDING ORGANIZATION–ENTERPRISE SYSTEM FIT: A PATH TO THEORIZING THE INFORMATION TECHNOLOGY ARTIFACT." MIS Quarterly **34**(4): 731-756.

US-CERT (2011). US-CERT Technical Information Paper – TIP-11-075-01, US-CERT.

Venkatesh, V. (2000). "Determinants of perceived ease of use: Integrating control, intrinsic motivation, and emotion into the technology acceptance model." Information Systems Research **11**(4): 342-365.

Wacker, J. G. (1998). "A definition of theory: research guidelines for different theory-building research methods in operations management." Journal of Operations Management **16**: 25.

Weber, R. (1987). Toward a theory of artifacts: A paradigmatic base for information systems research. Journal of Information Systems. **1:** 3-19.

Weir, C. S., G. Douglas, et al. (2009). "User perceptions of security, convenience and usability for ebanking authentication tokens." Computers & Security **28**: 47-62.

Whitten, A. and J. D. Tygar (1998). Usability of Security: A Case Study**:** 39.

Whitten, A. and J. D. Tygar (1999). Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0. 8th USENIX Security Symposium.

Yee, K.-P. (2004). "Aligining Security and Usability." IEEE Security & Privacy **5**(2): 48-55.

Zurko, M. E. and R. T. Simon (1997). User-Centered Security. New Security Paradigms.

Vita

Santa Ram Susarapu is a native of India where he was born and raised in the state of Andhra Pradesh. He graduated with a Bachelor of Commerce degree from Andhra University, Waltair in 1995. He came to the United States in 2000 to further his higher education and obtained Master of Business Administration from the University of Nebraska in 2003.

Santa Ram is currently working as a Senior Associate in KPMG's Risk Consulting practice in San Francisco, CA. Prior to joining KPMG in October 2010, Santa Ram worked as a seasoned IT audit professional for four years together in the Internal Audit Departments of Federal Home Loan Mortgage Corporation (Freddie Mac) and Genworth Financial, Inc. Santa Ram is a Certified Information Systems Security Professional (CISSP), a Certified Information Systems Auditor (CISA) and a Fellow-Life Management Institute (FLMI).