INFORMATION SYSTEMS MANAGEMENT MATURITY AND INFORMATION TECHNOLOGY SECURITY EFFECTIVENESS

GARRY SPICER

Bachelor of Science (Computer Science, IMS)

University of Ottawa, 1992

A Research Project
Submitted to the School of Graduate Studies Council
of the University of Lethbridge
in Partial Fulfillment of the
Requirements for the Degree

MASTER OF SCIENCE IN MANAGEMENT

Faculty of Management
University Of Lethbridge
LETHBRIDGE, ALBERTA, CANADA

INFORMATION SYSTEMS MANAGEMENT MATURITY AND

INFORMATION TECHNOLOGY SECURITY EFFECTIVENESS

GARRY SPICER

Approved:

Supervisor: Helen Kelley, Ph.D.	Date
Co-Supervisor: Brian Dobing, Ph.D.	Date
External Examiner: Mike Chiasson, Ph.D. University of Calgary, Calgary, Alberta	Date
Chair, Project Examination Committee: Michael Basil, Ph.D.	Date

Abstract

Modern societies rely on Information Systems (IS), yet their protection has long been considered ineffective. Researchers and practitioners have struggled to understand the persistence of this phenomenon, but both agree that IS management plays a significant role. This paper investigates the relation between practitioners' perceptions of IS management maturity and their perceptions of the effectiveness of Information Technology (IT) security. A cross-sectional survey (N = 68) was conducted to assess these perceptions. Analysis using Partial Least Squares provided evidence of a strong relation between these variables. Specifically, the perceived maturity of IS planning, control, and organization practices was positively associated with the perceived effectiveness of IT security. The relation between perceived maturity in IS management practices and perceived effectiveness of IT security is discussed, along with contributions to research and implications for practice. Limitations and directions for future research are presented.

TABLE OF CONTENTS

List of Tables

List of Figures

Introduction

Despite the extensive dependence of our society on Information Systems (IS), there is considerable evidence that Information Technology (IT) safeguarding is ineffective (Anthes, 1998; Brancheau, Janz, & Wetherbe, 1996; Christie & Goldman, 2003; *Global information security survey 2002*, 2002; Kankanhalli, Tan, Teo, & Wei, 2003; Keefe, 2003; Straub, 1990b; Straub & Welke, 1998; Verton, 2002). Furthermore, poor IT security is not a recent problem. It was noted in the late 1960s that the security of IT assets was often inadequate (Allen, 1968). Over time, several authors have proposed reasons for the persistence of this phenomenon, including: lack of knowledge on the part of IS managers, senior management, and end users; lack of tools for security managers and system administrators; lack of incentives for senior management to invest in IS security; and a general lack of interest from managers and end users (*Global information security survey 2002*, 2002; Goodhue & Straub, 1991; Kankanhalli et al., 2003; Loch, Carr, & Warkentin, 1992; Machefsky, 1998; Spafford, 1989; Straub & Welke, 1998). However, these reasons are either questioned by other researchers (Gollman, Meadows, & Okamoto, 2001) or, individually, provide low explanatory power (Goodhue & Straub, 1991).

Academic and practitioner literatures provide further reason to doubt that lack of knowledge, tools, incentives, or interest is entirely responsible for the low level of success in securing IS. First, knowledge about, and tools for, effective IT security management are available (Straub, 1986b; Trcek, 2003) and much has been written about effective approaches to IT security (Anthes, 1998; Dhillon, 2001; Gollman et al., 2001; Kankanhalli et al., 2003; Landwehr, 2001; Loch et al., 1992; Straub, 1990a; Straub &

Welke, 1998). Also, as Cheswick and Bellovin (1994) point out, good security principles, on which tools can be based, have been known for more than one hundred years. Security for IT is known to be both necessary and cost effective (Dhillon, 2001; *Global information security survey 2002*, 2002; Power, 2002; Straub, 1986a, 1990a, 1990b; Straub & Welke, 1998; Wood, 1987). It has even been noted that good security practices can lead to improvements in overall efficiency (Austin & Darby, 2003). Finally, interest in IT security is evident from the amount of material appearing in both academic and practice literatures (Backhouse & Dhillon, 1996; Briney & Prince, 2002; Gollman et al., 2001; Goodhue & Straub, 1991; Straub, 1986b; Troutt, 2002). So, a lack of knowledge, tools, incentives, or interest does not appear to adequately explain the enduring deficiencies in IT security. Despite ongoing efforts, both researchers and practitioners consider security for IT to be ineffective, resulting in calls for further investigation (Dhillon, 2003; Gollman et al., 2001; Kankanhalli et al., 2003; Straub & Welke, 1998).

While the knowledge and tools may be available, this does not mean that effective IT security is easily achieved. Misidentification of the problem, underestimation of the requirements, and lack of rigour in implementing solutions can undermine security efforts.

First, IT security may be misidentified as a purely technical, operational concern. However, several authors have pointed out that IT security is fundamentally a management problem, rather than a technical matter (Eloff, 1988; Ross & Weill, 2002; Trcek, 2003; Wood, 1987; Wylder, 1992). Loch et al. (1992) notes that it is IS managers who are responsible for understanding, and addressing, the threats to an organization's IT

assets. While there are technological implications, effective IT security is a management concern.

Second, it is possible to underestimate IT security requirements. One author points out that IT security is "extraordinarily complicated" (Austin & Darby, 2003, p. 120). The international standard *Code of Practice for Information Security Management* (*ISO/IEC 17799:2000*, 2000) specifies nine major areas of effective security practice (Organizational security, Asset classification and control, Personnel security, Physical and environmental security, Communications and operations management, Access control, Systems development and maintenance, Business continuity management, and Compliance). Another author (Daughtrey, 2001) highlights eight critical success factors for information security management. Among these are the need for an approach to security that is consistent with corporate culture, has visible support from management, and offers adequate security-related training and education for the organization's personnel. Thirteen separate dimensions of effective IT security have also been identified (von Solms, 2001). These include strategic governance, organizational governance, policy, best practices, ethics, certification, legal, insurance, personnel, awareness, technical, metrics, and audit aspects of IT security management. The complexity of this multifaceted issue is easily underestimated, and addressing the diverse aspects of IT security in modern organizations is a non-trivial undertaking.

Third, insufficient rigour can be an impediment to effective IT security. Safeguards are subject to a weak-link phenomenon (Neumann, 1996; Vasishtha, 2002). That is, the net effectiveness of any set of safeguards is constrained by the least effective member of the set, and as such, a single weak point can invalidate any or all of an

organization's security safeguards. As a corollary, it can be demonstrated that satisficing is a futile strategy for IT security. That is, implementing only part of a required set of safeguards may be no more effective than implementing none of the set. This principle can be applied recursively, so that even minor oversights in the implementation of an individual safeguard may seriously compromise its effectiveness, and in turn, an organization's entire IT security strategy.

In the face of these three issues, the possibility arises that even if knowledge, tools, incentives, and interest are present, they may not be adequate to ensure the effectiveness of IT security safeguards. Even if management is convinced of the need for IT security, the level of rigour required to properly apply the knowledge and tools can undoubtedly exceed that at which an organization normally conducts its affairs. Ultimately, the problem may simply be more difficult than many organizations are prepared to cope with.

In a recent study, Kankanhalli et al. (2003) developed and tested an integrative model of IS security effectiveness. The authors examined the influence of three organizational variables (organizational size, top management support, and industry type) and three mediating, management activity variables (deterrent efforts, deterrent severity, and preventive efforts) on the effectiveness of IT security. They found significant relations between the organizational variables and the management activity variables, and in turn, between the management activity variables and the effectiveness of IS security. Their findings imply that organizational factors, such as management support, and management actions, such as the use of deterrents and preventives, can influence the effectiveness of IT security.

Building on the integrative model of Kankanhalli et al. (2003), which theorizes that organizational factors can influence IT security effectiveness, this study will examine the influence of IS management maturity, as an organizational factor, on IT security effectiveness. Using the operationalization of IT security effectiveness implemented by Kankanhalli et al. (2003), this study examines how IS practitioners' perceptions of sophistication in IS management practices relate to their perceptions of the effectiveness of IT security safeguards. The need for managerial involvement in IT security, combined with the complex and exacting efforts required to effectively protect IT assets, suggests that a relatively sophisticated approach to IS management may be required to ensure effectiveness in IT safeguarding. IS practitioners, as a group, should be informed about both IS management practices and the effectiveness of IT security safeguards. As such, their perspectives offer a useful means of assessing these two variables.

IS management maturity has been used to characterize the sophistication of an organization's IS management practices, and the effectiveness and creativity with which those practices are applied (Karimi, Bhattacherjee, Gupta, & Somers, 2000). As organizations mature in their use of IS, management becomes increasingly aware of its strategic value, motivating their participation in overseeing the related systems, services, and data (Boynton & Zmud, 1987). The resulting changes in IS management may then alter the organization's ability to perceive security deficiencies, determine remedies, correctly implement solutions, and ensure continuing protection. Raho, Belohlav, and Fiedler (1987) imply such an effect in their discussion on the diffusion of personal computers. Additionally, in their study on the effectiveness of IT security, Kankanhalli et al. (2003, p. 152) suggests "organizational maturity" as a potential influencing factor.

Finally, a correlation has been demonstrated between IT management sophistication[1] and perceived success with IT (Sabherwal & Kirs, 1994).

The rest of this chapter provides an overview of IT security effectiveness, followed by an historical account of the development of the IS management maturity construct. The chapter concludes with a description of the research question and hypothesis.

IT Security Effectiveness

While the notion of security implying protection from the undesirable is intuitive, to measure its effectiveness in an organization's IT requires a more precise description. Definitions used in the academic literature, while precise, have tended to be narrow in their scope. To address this limitation, a broader characterization that is more reflective of typical industry norms will be used.

IT security effectiveness is conceptualized in this study as the extent to which security safeguards are perceived as successfully protecting IT-related hardware, software, data, and services from deliberate, accidental, or random threats to confidentiality, integrity, or availability. This includes physical, electronic, personnel, and policy safeguards. This is the definition used in this study's survey (see Appendix A).

[1] IS management maturity and IS management sophistication are used interchangeably in the literature.

To establish this definition of IT security effectiveness, four aspects of IT security will be examined here:

- Threats to IT (deliberate, accidental, and random);
- Types of IT assets requiring protection (hardware, software, data, and services);
- Types of IT compromises (confidentiality, integrity, and availability); and
- Types of safeguards (physical, electronic, personnel, and policy).

Threats to IT

Considering sources of threat, some authors apply a limited range of possibilities. IT security is sometimes defined as protecting IT assets only from intentional misuse (Kankanhalli et al., 2003; Straub, 1990b). In this definition, IT security is restricted to preventing people with malicious (or at least mischievous) intent from deliberately exploiting vulnerabilities to cause harm. However, this meaning is constrained with regards to the possible threats involved. Random events and human errors can also lead to security compromises (Morton & Froh, 1996).

A broader perspective on IT security threats is provided in the definition used by the Canadian Government. In its view, threats are defined as including "…malicious persons or groups, negligent or careless personnel, or … random occurrences and natural phenomena" (*A guide to risk assessment*, 1996, p. 8). This perspective includes threats that originate from deliberate, accidental, and random causes.

If threats include deliberate, accidental, and random sources, then each of the following events could be a security-related compromise:

- A terrorist attack that disables or destroys systems that support critical infrastructure;
- Unauthorized modification of payroll data by a dishonest employee;
- An accidental posting of personal information to a public web site in violation of privacy regulations;
- A random hardware failure in a network security device that results in sensitive systems being exposed directly to the public Internet;
- A weather-related electrical power failure that shuts down or damages vital systems.

For the purposes of this study, the conceptualization of security effectiveness will include deliberate, accidental, and random threats.

Types of IT assets requiring protection

Straub (1986b, p. 27; 1990a, p. 47; 1990b, p. 257) and Kankanhalli et al. (2003, p. 145) use the same scheme to describe IT assets that require protection, and this approach will be used in this study. The four IT assets are:

- *Hardware*: Any IT asset that can be physically touched by a human, such as computers, printers, network devices, and portable media (e.g., diskettes).
- *Software*: An IT asset that provides instruction sequences to control actions performed by IT hardware.

- *Data*: Data are an IT asset that consists of electronic representation of facts or knowledge.

- *Services*: A computer service is an IT asset that provides the capability to store, process, or transfer data. IT hardware and software assets work together to provide IT services. Examples of IT services include file and print capabilities, electronic mail, and Internet web access.

The conceptualization of security effectiveness in this study includes the need to protect the four IT asset types (hardware, software, data, and services).

Types of IT compromises

An organization's IT security policy states management's position on acceptable and unacceptable uses of IT assets, thereby defining *what* constitutes a security compromise. The Canadian government lists four types of IT compromises, including "replacement value" (the effective cost of replacing an asset if it were lost, damaged, or destroyed) as an asset sensitivity (*A guide to risk assessment*, 1996). Since this is essentially a consequence of a loss of availability, it will not be discussed further in this paper.

The realm of possible types of IT compromises can be grouped into a set of three different generic types of compromise (*A guide to risk assessment*, 1996):

- *Confidentiality*: Sensitivity to improper disclosure. Unauthorized access to and copying of data are examples of compromise to confidentiality.

- *Integrity*: Sensitivity to loss of accuracy or completeness. Data corruption and unauthorized changes to services are examples of integrity compromises.
- *Availability*: Sensitivity to loss or disruption of access to IT assets. Deliberate interference with computer services and destruction of hardware are examples of compromise to availability.

Kankanhalli et al. (2003) discusses various consequences of security compromises, such as financial losses and negative publicity. However, that study does not clearly define different generic types of compromises. For the purposes of this study, the conceptualization of security effectiveness will specifically include the need to protect against compromises of confidentiality, integrity, and availability.

Types of safeguards

The nature of the safeguards used to provide security must also be defined. A number of typologies have been developed for categorizing different types of safeguards. A four-component set (physical, electronic, personnel, and policy safeguards) is capable of encompassing a variety of schemes. Table 1 provides a comparison of the four safeguard types used in this study with other common typologies.

The four safeguard types used in this study are defined here as:

- *Physical*: Safeguards such as locks, shields, fire suppression, and guards that provide protection for tangible IT assets.
- *Electronic*: Safeguards such as passwords, firewalls, and file access controls that restrict access to, or use of, data or services.

- *Personnel*: Safeguards such as background checks, security awareness activities, and training that attempt to reduce threats from internal personnel.
- *Policy*: Safeguards such as security or operations policies, guidelines, standards, practices, and procedures that explain management's position on acceptable and unacceptable uses of IT assets.

Table 1 Comparison of safeguard typologies used in various studies

Safeguard type	(Straub, 1990a) equivalent term(s)	(Straub, 1990b) equivalent term(s)	Government of Canada equivalent term(s) (A guide to security risk management, 1996)	Government of Canada equivalent term(s) (A guide to risk assessment, 1996)
Physical	Physical	Physical	Non-technical: physical	Physical and environmental, hardware
Electronic	Programmed	Electronic	Technical	Hardware, software, communications, transmission, cryptographic, emission, network
Personnel	N/A	N/A	Non-technical: personnel	Personnel
Policy	Administrative	N/A	Non-technical: procedural	Administrative and organizational, operations

While Kankanhalli et al. (2003) discusses various ways of classifying IT safeguarding practices, the authors do not explicitly define types of IT security

safeguards in their study. For the purposes of this study, the conceptualization of security effectiveness will include the use of the four safeguard types presented here: physical, electronic, personnel, and policy.

Conceptualization of IT security effectiveness

Summarizing the above discussion of both academic and industry definitions, IT security effectiveness is conceptualized in this study as the extent to which security safeguards are perceived as successfully protecting IT-related hardware, software, data, and services from deliberate, accidental, or random threats to confidentiality, integrity, or availability. This includes physical, electronic, personnel, and policy measures.

Additionally, Kankanhalli et al. (2003) examined overall preventive and deterrent effects of IT security safeguards in the study's integrative model. While not reflected in the definition of IT security effectiveness used here, these safeguard protection classes are also examined in this study to remain consistent with the model used by Kankanhalli et al. (2003). Preventives and deterrents are further discussed in the following section, in context with other safeguard protection classes, such as detection, containment, and recovery.

Safeguard protection classes

Safeguards can be classified based on the manner in which they support an organization's security policy. A safeguard may be invoked at one or more of several points in a potential or actual compromise scenario, depending upon whether the intent is to avert a compromise before it happens, identify or inhibit a compromise in progress, or deal with the results of a compromise, after the fact. Physical, electronic, personnel, and policy safeguards can be implemented in variety of modes, depending upon the point in a compromise scenario at which it should be invoked. Table 2 compares a number of protection classification schemes.

Table 2 Comparison of safeguard classification schemes

Safeguard protection class	(Kankanhalli et al., 2003) equivalent terms	(Straub, 1990b) equivalent term(s)	(Straub & Welke, 1998) equivalent term(s)	Government of Canada equivalent term(s) (*A guide to risk assessment*, 1996, p. 22)	(Morton & Froh, 1996) equivalent term(s)
Deterrence	Deterrent measures	Deterrent	Deterrent	Deterrence	Threat motivation
Prevention	Preventive measures	Preventive	Prevention	Prevention and avoidance	Preventative
Detection	N/A	N/A	Detection	Detection	Detective
Containment	N/A	N/A	N/A	Mitigative	Containment
Recovery	N/A	N/A	Remedies	Mitigative	Recovery

The five safeguard classes outlined in Table 2 are capable of covering all components of the four classification systems shown in the table. Extending the meanings used in previous research (Straub & Welke, 1998), these classes are defined as:

- *Deterrence*: These safeguards attempt to discourage deliberate attacks against a system through dissemination of information and threat of sanction. This class includes components such as penalties for violations of security policies and security awareness training. It can be argued that deterrent techniques are also useful in avoiding certain types of accidental threats, by educating personnel about the need for extra care and attention in security matters.

- *Prevention*: These safeguards impede security violations by actively enforcing aspects of the organization's security policy. Attempts to violate an aspect of policy enforced by a preventive safeguard are denied or inhibited by the safeguard itself. This occurs regardless of whether the attempted violation is due to deliberate or accidental actions. Door locks, file access controls, and passwords are examples of this class.

- *Detection*: Detection involves determining when a security violation has occurred. This situation generally arises when the security policy (a deterrent) has been disregarded and safeguard mechanisms (a preventative) have been circumvented or overcome. Detection is only useful if it triggers a response, so this definition can be extended by creating sub-classes of real-time and post-hoc detection techniques. Real time detection techniques, such as Intrusion Detection Systems (IDS) and network monitoring are intended to

elicit rapid reactions to threats. Post hoc detection techniques, such as security investigations, and suspicious activity reports are designed to "gather evidence of misuse and to identify perpetrators" (Straub & Welke, 1998, p. 446). These methods also provide information for post mortem analyses to aid in better management of future incidents.

- *Containment*: These safeguards are intended to "limit the injury that would occur if a threat event is successful" (Morton & Froh, 1996, p. 191). A containment safeguard is used to ensure that a partial compromise does not immediately imply a total compromise. For example, the use of offsite backups ensures that a fire in one building does not cause the simultaneous destruction of data on both the main system and backup media.

- *Recovery*: Recovery safeguards involve follow-up actions after a successful threat event. For deliberate threats, this can include punishment of offenders, through reprimands, termination, or legal action. This can have the effect of recovering public confidence or recovering direct damages in a lawsuit. Recovery can also include any actions taken to restore the integrity or availability of IT assets (e.g., restoring lost or damaged files).

Not all of these schemes presented in Table 2 consider the detection, containment, and recovery safeguard classes. However, all address both deterrents and preventives as key aspects of security safeguarding. These two classes have the benefit of rigorous investigation (Gopal & Sanders, 1997; Straub, 1986b), and a basis in general deterrence

theory[2] (Straub, 1990b; Straub & Welke, 1998). This study will specifically examine the use of deterrent and preventive class safeguards by assessing their perceived overall effectiveness (Appendix A, Q14 - Q17). This is consistent with the integrative model used by Kankanhalli et al. (2003). The examination of these safeguard classes does not alter the conceptualization of IT security effectiveness in this study, but provides an additional perspective of IS practitioners' perceptions of the effectiveness of IT safeguards.

IS Management Maturity: An Historical Overview

The IS management maturity research construct has undergone several iterations and revisions over the past 30 years, as researchers grappled with its complex nature. Works of specific interest to this study include the following:

- The initial suggestion of a staged progression in IS management maturity levels (Churchill, Kempster, & Uretsky, 1969);
- Nolan's (1973) original four-stage IS maturity model;
- Gibson and Nolan's (1974) refinement of the model;
- Nolan's (1979) second, six-stage model;
- A series of criticisms of the stage model approach (Benbasat, Dexter, Drury, & Goldstein, 1984; Drury, 1983; King & Kraemer, 1984; Lucas & Sutton, 1977); and

[2] Deterrence theory, part of the field of criminology, proposes that antisocial acts can be deterred through the application of compelling dissuasive measures and serious penalties for committing undesirable acts (Straub & Welke, 1998, p. 445).

- A set of alternative or refined approaches to modeling IS management sophistication (Auer & Ruohonen, 1997; Benbasat, Dexter, & Mantha, 1980; Farhoomand & Gatehouse, 1988; Galliers & Sutherland, 1991; Karimi, Gupta, & Somers, 1996; Sabherwal & Kirs, 1994).

While the genesis of IS management maturity theory can be traced to earlier material (Churchill et al., 1969), Richard Nolan (1973) is generally credited with first expressing the notion that an organization's IS management approach progresses through a series of four stages (Initiation, Contagion, Control, and Maturity). Gibson and Nolan (1974) soon refined this model to further describe the processes that occur throughout each of the stages. Nolan (1979) later expanded the model to include six stages (Initiation, Contagion, Control, Integration, Data Administration, and Maturity). Both models used variations on IS budget growth as a predictor for IS management maturity. These models have been called "…among the best known ideas in MIS" (Drury, 1983, p. 59), with the Gibson and Nolan (1974) work being one of the most cited articles in MIS research (Galliers & Sutherland, 1991).

Despite the popularity of Nolan's stage theory, critics have pointed out that:

- The initial model was based on anecdotal data rather than scientific analysis, and IS budget alone is inadequate to predict maturity (Lucas & Sutton, 1977);
- The models are an oversimplification, and do not accurately predict the erratic behaviour often exhibited by real organizations (Drury, 1983; King & Kraemer, 1984);

- Over time, an organization's experience with IS becomes progressively less predictable and more idiosyncratic (Sullivan, 1985);
- The models imply that maturity is a one-dimensional, monotonically increasing function (Benbasat et al., 1984; Sullivan, 1985); and
- Technology dependencies in the models (e.g., database systems) can render them outdated for certain uses (Galliers & Sutherland, 1991; Sullivan, 1985).

Nonetheless, most critiques also concluded that there was no evidence to clearly invalidate the general aspects of maturity theory. Furthermore, the notion of IS management maturity finds acceptance in both the research and practitioner communities (Drury, 1983; Galliers & Sutherland, 1991; King & Kraemer, 1984). One study provides an explanation for the appeal of this idea among practitioners:

> It is because it provides a conceptual language enabling an IS manager to identify where his/her firm is positioned in a "stages" sense. This allows the manager to better grasp the current challenges facing the firm and the appropriate tactics for overcoming them, to predict what is likely to happen as the firm transcends to successive stages, and most importantly, to communicate these notions to other executives. (Benbasat & Zmud, 1999, p. 11)

In response to the limitations of Nolan's theory, alternate models for defining and measuring IS management maturity or sophistication have been proposed (Auer & Ruohonen, 1997; Farhoomand & Gatehouse, 1988; Galliers & Sutherland, 1991; Sabherwal & Kirs, 1994). Related work in IS management maturity (Benbasat et al., 1984; Benbasat et al., 1980) and technology assimilation (McFarlan, McKenney, & Pyburn, 1983), was later used by Karimi et al. (1996) to develop a multi-item, multi-

dimension model to measure IS management maturity. Where Nolan's original work (1973) used three categories (planning, controlling, and organizing) to describe activities in the four maturity stages, a more recent model (Karimi et al., 1996, p. 64-65) uses the following four dimensions:

- *IT Planning Mode*: Alignment of IT with the business, and use of managerial planning for improving the use of IT throughout the organization.
- *IT Control Mode*: Use of a managerial orientation toward measuring IT value, basing controls on benefits, priorities, and standards.
- *IT Organization*: Roles and responsibilities of users and IT personnel, and the level in the organization at which IT management resides.
- *IT Integration*: Use of top down planning for IT, increased technology transfer, and greater exploitation of technology throughout the firm.

The Karimi et al. (1996) model has been applied successfully in several recent studies that examine the maturity of an organization's IS management function. The first of these studies (Karimi et al., 1996), a survey of IT managers in the American financial services industry, examined the effect of IS management maturity factors (planning, control, organization, and integration) on a firm's response to market globalization. This study found that higher scores on the control, organization, and integration factors were associated with increased spending on IT in the context of international free trade agreements. Another study (Gupta, Karimi, & Somers, 1997) looked at differences in IS management maturity factors based on a firm's competitive strategy. Using the Miles

and Snow (1978) framework of Prospectors, Analyzers, Defenders and Reactors, this study found that firms using different strategies tended to differ in their emphasis on the four maturity factors. A third study (Karimi et al., 2000) investigated relations between the use of IT steering committees in organizations and IS management maturity factors. The authors found that the presence of IT steering committees correlated positively with higher levels of IS management maturity, and that that the type of steering committee predicted which of the maturity factors would dominate. Finally, Karimi, Somers, and Gupta (2001) looked at differences in IS management maturity factors based on a firm's customer service technology. The results demonstrated that improvements in customer-service can be related to increasing levels of the four IS management maturity factors.

There are several reasons why the approach used by Karimi et al. (1996) is particularly suitable for measuring IS management maturity in the study described in this paper. First, the model is simple and parsimonious, rendering it easy to explain, understand, and apply. Second, it provides validated constructs that can be used for either longitudinal or cross-sectional comparisons. Third, it comprises a multiple-item measurement that captures enough factors to provide a useful conceptualization of the notion of IS management maturity. Fourth, the model is independent of technology-specific constructs, and is therefore applicable regardless of the technology in use. Fifth, the model inherently accounts for the need to address internal and external factors that can affect the IS management maturation process, by measuring variables that deal with goals, planning, and communication as these relate to internal and external actors. Thus, this model has the flexibility to incorporate change, in terms of new strategies and planning requirements. Finally, while implying that cycles of maturity (i.e., the four

phases) occur whenever new technologies are introduced, the model does not require a monotonic progression through those phases.

One potential criticism of maturity models is the implication that there is one 'ideal' level of maturity for all organizations, and therefore, a rigid notion of one 'best' way of managing IS for all possible situations. However, the meaning of maturity in the Karimi et al. (1996) model reflects the extent to which IS is incorporated into the organization, and is able to effectively use resources to meet organizational requirements. Thus, the model's flexibility is increased by emphasizing generic IS management activities, rather than implementation details that may vary from one organization to another. This also maintains the model's usefulness in cross-sectional analysis, since it is possible to make meaningful comparisons of the degree to which an IS group is involved within an organization, aware of the organization's needs, and able to effectively use existing resources.

Research Question and Hypothesis

No research has been found that explores the relation between IS management maturity and IT security effectiveness. The objective of this study is to examine how IS practitioners' perceptions of IS management maturity relate to their perceptions of the effectiveness of IT security. To do this, this study will test the following research hypothesis, as depicted in Figure 1:

- *H1*: Perceived IS management maturity (measured by planning, control, organization, and integration components) positively correlates with perceived IT security effectiveness.

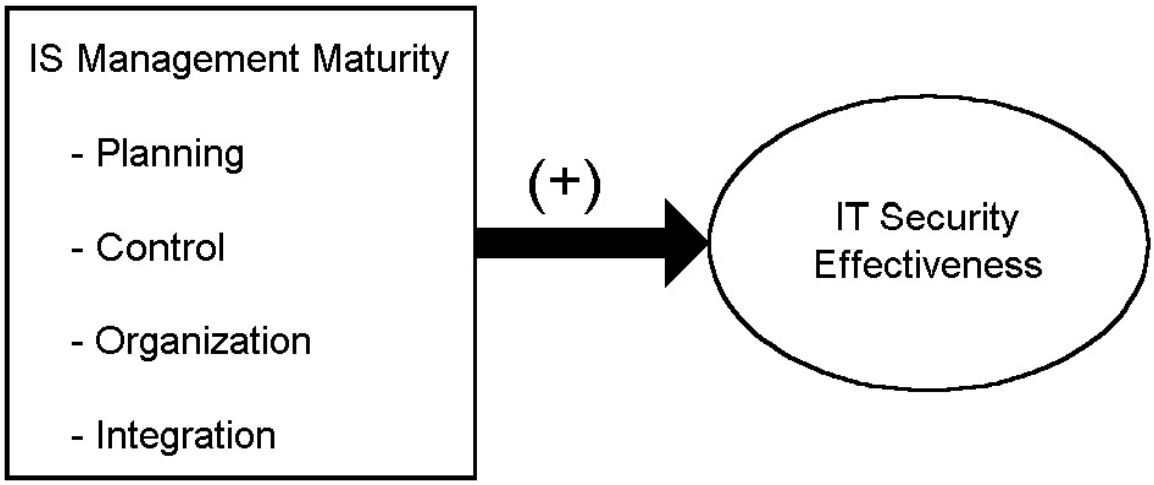


Figure 1. IS management maturity and IT security effectiveness research model.

Method

This study's research question is examined with a quantitative methodology using a cross-sectional survey design. The targeted population is English-speaking IS practitioners in Canada. The sample frame is based on IS practitioners who were members of selected Canadian IS associations at the time of the study. The survey was implemented as an Internet web site.

The primary constructs of the survey, IT security effectiveness and IS management maturity, are based on Kankanhalli et al. (2003), for IT security, and Karimi et al. (1996), for IS management maturity. Components of the previously validated instruments of these researchers were reused to reinforce the validity of this study. A series of pre-testing activities were undertaken to validate the survey instrument and the project was subjected to an ethics review prior to any contact with participants. Participants were solicited by way of their associations' electronic mailing lists. The following sections examine each of these matters in further detail.

Population and Sample Design

This study used an individual unit of analysis, which helped to improve sample size. Additionally, substantial variations can exist within an organization (Sullivan, 1985). So, it is reasonable to assume that irregularities may also exist in IS management practices and IT security effectiveness across an organization's IS infrastructure. Examining the perceptions of individuals improves the capture of such differences.

Respondents had to be capable of answering questions about IS management and IT security. Since increasing levels of computer literacy are associated with greater

awareness of IT security issues (Goodhue & Straub, 1991), end-users and other non-IS personnel are unlikely to respond well to security questions. IS practitioners, though, are likely to be informed about, and influential concerning, both IS management practices and IT security safeguards. Their perspective should provide useful insights on the subject (Goodhue & Straub, 1991). IT security specialists, as a subset of the IS practitioner population, would be particularly well informed respondents. However, this population is small in Canada. Since the original source instruments were written in English, it was felt that respondents' language of business should be the same. English speaking, Canadian IS practitioners were therefore selected as the target population of this study. This population does include a significant number of IT security specialists, which is in keeping with previous studies in this area (Goodhue & Straub, 1991; Straub, 1990b).

The population selected for this study is broader than that used by Karimi et al. (1996) to investigate the effects of IS management maturity on a firm's response to market globalization. Their survey was sent only to IT managers in the American financial services sector. While the Kankanhalli et al. (2003) survey of IS security effectiveness did encompass a range of industries, it was still restricted to IS managers who belonged to an unnamed industry association. By examining the perceptions of IS practitioners of various specializations across diverse industry segments, this study is able to capture a broader range of relevant perspectives. The responses of a more heterogeneous population also provide a more demanding test of the research hypothesis, since surveying only managers, particularly if from a single industry, may reflect a narrower view of the issue.

Since IS is not a regulated profession in Canada, there is no known complete list of IS practitioners and no certain means of selecting a random sample of potential participants from this population. The best available sample frame was considered to be the members of Canadian IS practitioner associations. Therefore, a convenience sample was used, based on membership in one of two Canadian IS practitioner associations, yielding a sample frame of about 5,000 practitioners.

Operationalization of Constructs

IT security effectiveness

Two approaches to operationalizing IT security effectiveness were found in the literature. One of these approaches (Goodhue & Straub, 1991; Straub, 1989, 1990b) measures rates of security abuse, and has many advantages, including a rigorously validated instrument. However, this approach has drawbacks. First, the questionnaire used by Straub seeks potentially sensitive information, including the number of security incidents experienced in an organization and the corresponding dollar loss consequences. Loch et al. (1992) notes that these types of queries are likely to inflate non-response, despite the fact that Straub (1990b) reports respondent reluctance to answer these questions was not an issue in that study[3]. Second, since many organizations do not maintain suitable records of actual security incidents, the measures are based on data that may not be accurately recorded (Kankanhalli et al., 2003). Even where such records may exist, they may not be readily accessible to a large portion of the survey sample frame.

[3] Straub's study achieved a 22% survey response rate.

This can lead to a variety of potential problems, including faulty recall and underreporting biases.

To address concerns over confidentiality and level of analysis, this study employs an alternative approach to measuring IT security effectiveness. Adapting earlier work (Straub, 1990b), Kankanhalli et al. (2003) employs a perceptual measurement to operationalize the sufficiency of IT security. The measurement is a six-item scale that includes components relating to the perceived adequacy of protection for IT hardware, software, data, and services, as well as overall deterrent and preventive effects. The reliability scores of these factors, as reported by Kankanhalli et al. (2003), are provided in Table 3. Based on pre-testing results, an expanded set of eight items (Appendix A, Q10 - Q17) was used to operationalize this construct. The items are summarized as follows:

- *Protection of hardware*: A single item measuring perceived effectiveness of security safeguards for IT related hardware.
- *Protection of software*: A single item measuring perceived effectiveness of security safeguards for IT related software.
- *Protection of data*: A single item measuring perceived effectiveness of security safeguards for electronic data.
- *Protection of computer services*: A single item measuring perceived effectiveness of security safeguards for computer services.
- *Overall deterrent effect*: The single item used to measure the perceived effectiveness of disincentives against deviant acts was split into two parallel items measuring deterrence separately for insiders and outsiders.

- *Overall preventive effect*: The single item used to measure the perceived effectiveness of preventive countermeasures was split into two parallel items measuring prevention separately for insiders and outsiders.

Table 3 Factor scores (Kankanhalli et al., 2003)

IT security effectiveness variable	Hardware protection	Software protection	Data protection	Services protection	Deterrent effect	Preventive effect
Reliability	.88	.80	.85	.83	.77	.75

IS management maturity

IS management maturity was operationalized by adapting the Karimi et al. (1996) 20-item instrument for measuring IS planning, control, organization, and integration. Table 4 provides reliability scores for these multi-item factors as reported in the Karimi et al. study. All factors presented Cronbach's Alpha scores of over .70, which is generally considered the minimum acceptable lower limit (Hair, Anderson, Tatham, & Black, 1998, p. 118). An adapted set of 21 items (Appendix A, Q41 – Q46, Q34 – Q39, Q28 – Q32, Q23 – Q26) was used in this study's survey. The following subsections provide descriptions of the four maturity factors.

Table 4 Factor reliability (Cronbach's Alpha) scores (Karimi et al., 1996)

IS maturity variable	Planning	Control	Organization	Integration
Reliability	.88	.86	.80	.78

Planning

Six items measure respondent's perceptions of the planning component of maturity. These items were designed to capture the extent to which the organization has been able to "align IT plans with … business plans and to extend the infusion and diffusion of IT…" (Karimi et al., 1996, p. 64). These items are presented in Section 3D of the survey instrument (Appendix A, Q41 – Q46).

Control

Six items measure respondent's perceptions of the control component of maturity. These items were designed to assess the organization's use of "controls … based on benefits, priorities (selective charge-out) and technical standards and the organizational goals …" (Karimi et al., 1996, p. 64). These items are presented in Section 3C of the survey instrument (Appendix A, Q34 – Q39).

Organization

Karimi et al. (1996) used four items to measure respondent's perceptions of the organization component of maturity. A fifth item (Appendix A, Q28) was added to this study's instrument after pre-test results demonstrated a potential response concern. (This item is discussed further in the later section on Instrument Development.) These items were designed to assess the degree to which the structure of the IS group fits with organizational needs and how well it is able to capture and process ideas. This is especially important with respect to the ideas of end-users, which require "special attention in the planning and implementation of applications" (Karimi et al., 1996, p. 64).

These items are presented in Section 3B of the survey instrument (Appendix A, Q28 – Q32).

Integration

Four items measure respondent's perceptions of the integration component of maturity. These items were designed to determine the organization's ability to link IS strategy to business needs, transfer technology to applications, and effectively exploit IT (Karimi et al., 1996, p. 65). These items are presented in Section 3A of the survey instrument (Appendix A, Q23 – Q26).

Implementation

The 21 items comprising the four dimensions of IS management maturity, and the 8 items measuring IT security effectiveness, were all implemented using a five-point Likert scale ranging from 1 (*strongly disagree*) to 5 (*strongly agree*). This same implementation was used by Karimi et al. (1996) for the IS management maturity items. However, the IT security items, as originally implemented by Kankanhalli et al. (2003), used a seven-point Likert scale that ranged from 1 (*strongly disagree*) to 7 (*strongly agree*). The security questions were therefore adapted to a five-point Likert scale to present a more consistent appearance to survey respondents. These two constructs provided a prevalidated set of measures for the independent and dependent variables under consideration.

Instrument Development

The survey was implemented as a web site, which was felt to be consistent with the characteristics of the targeted respondents. It can reasonably be assumed that this group has experience in computer-related technologies, so novelty effects of a web-based instrument were not seen as significant. This approach also permitted measurement of individuals' perceptions from a large, geographically dispersed sample frame in a short period of time, while controlling costs.

Following procedures recommended by Dillman (2000), several stages of pre-testing were undertaken before the survey was released. These are presented in the following subsections.

Stage one

Dillman (2000) suggests beginning the instrument pre-testing process with reviews by knowledgeable colleagues. The project research committee served in this capacity, thoroughly reviewing the instrument and refining it several times before proceeding to the next stage of pre-testing.

Stage two

Using a combination of Dillman's (2000) Concurrent Think-Aloud Protocol and Retrospective Interview techniques, the instrument was pre-tested in a paper form with four different IS practitioners. The individuals involved ranged in experience from a junior technical level to a senior managerial position. Thus, it was possible to estimate how practitioners of different seniority levels might respond to the questions. Wordings

were changed to reduce ambiguity in several items as a result of difficulties noted by the pre-test subjects. Additionally, the two security effectiveness items concerning deterrence and prevention were split into four items so that an insider/outsider[4] dichotomy could be included. Finally, one additional item (Appendix A, Q28) was added to the organization factor of IS management maturity to capture the extent to which the ideas of IT personnel are included in IT planning and implementation. The original questions and their adapted versions are presented in Table 5 through Table 10.

[4] Pre-testing indicated that field practitioners often distinguish between safeguarding against "insider" and "outsider" based compromises. Insiders are generally considered to be persons who are known to the organization and therefore have first-hand knowledge of the organization's operations. Outsiders do not generally have such information readily available to them.

Table 5 Comparison of IT security effectiveness items

Item from Kankanhalli et al. (2003)	Adapted item
The computer security effort is very effective in protecting the following from abuse:	
Hardware	At your primary place of work, current Information Security measures provide effective protection for **IS hardware**:
Software	At your primary place of work, current Information Security measures provide effective protection for **IS software**:
Data	At your primary place of work, current Information Security measures provide effective protection for **electronic data**:
Computer services	At your primary place of work, current Information Security measures provide effective protection for **the services provided by information systems** (e.g. file, print, email services):

Table 6 Comparison of IT security safeguard protection class items

Item from Kankanhalli et al. (2003)	Adapted item
The computer security effort is very effective in protecting the following from abuse:	
Overall deterrent effect	At your primary place of work, current Information Security measures are effective in **deterring** security violations by **insiders** (i.e. discouraging **known/internal people** from attempting to breach the organization's security measures):
	At your primary place of work, current Information Security measures are effective in **deterring** security violations by **outsiders** (i.e. discouraging **unknown/external people** from attempting to breach the organization's security measures):
Overall preventive effect	At your primary place of work, current Information Security measures are effective in **preventing** security violations by **insiders** (i.e. stopping attempts by **known/internal people** from actually breaching the organization's security measures):
	At your primary place of work, current Information Security measures are effective in **preventing** security violations by **outsiders** (i.e. stopping attempts by **unknown/external people** from actually breaching the organization's security measures):

Table 7 Comparison of planning maturity items

Item from Karimi et al. (1996)	Adapted item
Our IT projects support the business objectives and strategies of our company.	At your primary place of work, the IT projects support the organization's business objectives and strategies.
We continuously examine the innovative opportunities IT can provide for competitive advantage.	At your primary place of work, the organization regularly examines the innovative opportunities that IT can provide for competitive advantage.
We are adequately informed on the current use of IT by competitive forces (e.g., buyers, suppliers, and competitors) in our industry.	At your primary place of work, the organization is adequately informed about the **current** use of IT by competitive forces (e.g. buyers, suppliers, and competitors) in its industry.
We are adequately informed on the potential use of IT by competitive forces (e.g. buyers, suppliers, and competitors) in our industry.	At your primary place of work, the organization is adequately informed about the **potential** use of IT by competitive forces (e.g. buyers, suppliers, and competitors) in its industry.
We have an adequate picture of the coverage and quality of our IT systems.	At your primary place of work, the organization has adequate information about the capabilities and quality of its IT systems.
We are content with how our IT project priorities are set.	At your primary place of work, the organization is satisfied with how its IT project priorities are set.

Table 8 Comparison of control maturity items

Item from Karimi et al. (1996)	Adapted item
In our organization, the responsibility and authority for IT direction and development are clear.	At your primary place of work, the overall responsibility and authority for IT direction and development are clear.
In our organization, the responsibility and authority for IT operations are clear.	At your primary place of work, the overall responsibility and authority for IT operations are clear.
We are confident that IT project proposals are properly appraised.	At your primary place of work, IT project proposals are properly appraised.
We constantly monitor the performance of IT functions.	At your primary place of work, the organization regularly monitors the performance of its IT functions.
Our IT function is clear about its goals and responsibilities.	At your primary place of work, the IT group is clear about its goals and responsibilities.
Our IT function is clear about its performance criteria.	At your primary place of work, the IT group is clear about its performance criteria.

Table 9 Comparison of organization maturity items

Item from Karimi et al. (1996)	Adapted item
N/A	At your primary place of work, the ideas of IT personnel are given due attention in IT planning and implementation.
In our organization, user ideas are given due attention in IT planning and implementation.	At your primary place of work, end user ideas are given due attention in IT planning and implementation.
Our IT specialist understands our business and the firm.	At your primary place of work, the IT personnel understand the business and the organization.
The structure of our IT function fits our organization.	At your primary place of work, the structure of the IT group fits the organization.
The IT specialist-user relations in our firm are constructive.	At your primary place of work, relations between IT personnel and end users are constructive.

Table 10 Comparison of integration maturity items

Item from Karimi et al. (1996)	Adapted item
In my firm top management perceives that future exploitation of IT is of strategic importance.	At your primary place of work, top management perceives that future use of IT is of strategic importance.
There is a top-down planning process for linking information systems strategy to business needs.	At your primary place of work, there is a top-down planning process for linking IT strategy to business needs.
Some IT development resource is positioned within the business unit.	At your primary place of work, some IT development resources are positioned within individual business units/functional areas/departments.
The introduction of, or experimentation with, new technologies takes place at the business unit level under business control.	At your primary place of work, the introduction of, or experimentation with, new technologies takes place at the business unit/functional area/department level under business unit/functional area/department control.

Stage three

Dillman (2000) recommends that a pilot study be undertaken at this point, to validate the procedures that are intended to be used in the main study. Due to time and sample restrictions, a full pilot study was not feasible. In its place, two rounds of additional pre-testing were performed once the instrument had been implemented in its electronic format. In the first round, the protocol used in stage two pre-testing was used to observe two participants responding to the survey questions in their electronic format. Based on the results of this round, the instrument was modified to improve the visibility of instructions, highlighting of keywords, and ease of navigation through the questions. In the second round of this stage, three additional IS practitioners responded to the electronic pre-test questionnaire, having only been provided with instructions via electronic mail messages. This closely emulated the procedure that was later used with respondents to the main study. No significant procedural problems were detected.

Stage four

Dillman (2000) suggests a final check, performed by people who have not been involved in the questionnaire development up to that point. This is considered important, since "People who have worked on one revision after another soon lose their ability to detect obvious problems" (Dillman, 2000, p. 147). A walk-through of the entire process was performed with one person, who had not been directly involved in the questionnaire development. No significant concerns were raised during this procedure.

Procedure

Research ethics approval

Prior to engaging any participants in this study, application was made to The Faculty of Management Research and Ethics Committee at The University of Lethbridge. This committee reviewed the proposed research design to ensure conformance to acceptable ethical guidelines and standards as described in the Tri-Council Policy Statement for the ethical conduct of research involving humans. Approval was granted before any contact was made with the study participants.

Solicitation of participants

Executive members from four different Canadian IS practitioner organizations were approached to determine if they would be willing to facilitate access to their membership for participation in this study. Two organizations did not respond and two agreed to send the solicitation notices to their members via electronic mailing lists. Citing privacy concerns, neither of the participating organizations would permit direct access to their membership lists.

The first of the two participating groups (Association 'A') is a large, national body of IS practitioners. This organization represents both IS generalists and a wide range of IS specialists from several provinces across Canada. Only those registered as English-speaking members from this group were contacted. A biweekly electronic newsletter was the only means of contact with members of this organization.

The second organization (Association 'B') is a smaller group of IS practitioners from a large Western Canadian city. This group consists primarily of practitioners whose focus is IT security and privacy matters. Solicitation notices were sent to this organization via an electronic mailing list and were timed to coincide with the notices sent to members of Association 'A.'

To bring attention to the study, a pre-notice was sent to both associations approximately two weeks before the survey web site was made available. Association 'B' published this pre-notice to their members, but Association 'A' did not. Additionally, approximately one week prior to the pre-notice, the executive of Association 'B' openly endorsed the survey during a regular meeting of the organization's membership. Once the survey web site became available, both associations published an announcement to their membership. Two weeks later, both associations also published a follow-up notice to their membership via the same electronic mail medium used for the pre-notice and announcement. The survey notices and announcement are presented in Appendix B. Approximately two weeks after the follow-up notices were published, the web site was closed and the database moved to a secure location for analysis.

Two actions were taken to help attract participants. First, those who completed the survey were given the opportunity to request a copy of the study's results. Second, participants could also optionally choose to participate in a draw for one of four $50 gift certificates from a popular retailer of office supplies and business technology. While there is some debate about the effectiveness of such measures, these two techniques are commonly used as survey participation incentives (Ilieva, Baron, & Healey, 2002).

Results

Association 'A' reported that approximately 5,000 people across Canada were registered to receive the English version of its electronic newsletter. The association also reported that approximately 17% of its members were students who would be unlikely (and arguably, unqualified) to respond to this survey. Thus, the overall sample frame, once unqualified respondents were removed, totaled approximately 4,150 potential participants. However, only 32 responses were received from this organization. Due to missing data (i.e. skipped questions or answers of 'not sure' – see section entitled Missing data for more details) 10 responses were removed, leaving just 22 useable responses. Individuals could not be contacted directly, so a precise response rate cannot be calculated, but this response is approximately 0.77%, with 0.53% being useable.

Web-based surveys are known to risk low response, with rates being up to 80% lower than their paper equivalents (Morrel-Samuels, 2003). However, this response is very low by any standard, suggesting that either distribution or readership may not be accurately reflected in the newsletter registration figure. In a conversation that took place a few months after the survey was complete, one member of this association mentioned that it was not uncommon for members to ignore the association's electronic newsletter as a means of dealing with time constraints and information overload. Thus, the effective sample frame size may have been very much smaller than originally anticipated. In any case, it seems unlikely that a lack of interest alone would account for the low response, since this association is known to have several, well-attended Special Interest Groups (SIGs) that focus primarily on IT security topics. Rather, one or more of several factors,

discussed in the following paragraph, may have negatively affected response from Association 'A.'

The low response from Association 'A' may be partially attributable to a pre-notice not being published as planned in the association's newsletter, due to the unexpected pre-announcement of another, unrelated survey on IT security. Members of Association 'A' may have confused the two pre-notices, and since the one for this project was the second to appear, many people may simply have ignored it. Lack of a pre-notice and limited response windows have been suggested as factors that can negatively affect response to web surveys (Ilieva et al., 2002). Time constraints permitted the survey web site to be active for only four weeks, so lack of a pre-notice could have delayed some responses beyond the time available for participation. Also, discussions with a second member of Association 'A' indicated that its newsletters frequently contain survey solicitations, so members may have succumbed to survey fatigue. This has been noted as a serious problem for response rates in web-based questionnaires (Couper, 2000). Finally, timing may be a major factor in the lack of response. It was necessary to perform data gathering activities during the summer, which has been suggested as a period during which response to electronic mail survey notifications can be seriously affected (Ilieva et al., 2002).

Association 'B' reported that the invitation to participate in the survey was distributed via their email list, and was sent to 325 people throughout Western Canada. A total of 66 responses were received from this organization. Due to missing data (i.e. skipped questions or answers of 'not sure' – see section entitled Missing data for more

details), 20 responses were removed, leaving 46 useable responses. This yielded a useable response rate of approximately 20%.

The higher response rate from Association 'B' is likely due to five factors. First, the primary focus of this group is IT security and privacy. Second, this group had not taken part in such surveys in the past, so survey fatigue is likely to be much less of an issue. Third, the association's executive actively endorsed the survey. Fourth, a survey pre-notice was sent to the members of this group. Finally, a brief presentation was made during one of the association's meetings to encourage participation.

Overall, response to this survey was considerably less than anticipated. Because of the low response rate and the use of a convenience sample, there are difficulties in generalizing the results to the broader population. Consequently, tests for response biases were not considered practical. Those who did participate, however, generally provided complete responses, often including detailed comments to explain their choices. These participants obviously took significant time to consider their responses and ensure that they were clearly understood. Thus, what is lacking in the quantity of data is somewhat offset by the high quality of the information obtained.

Participant Profile

Demographic results describing the personal attributes of survey respondents are presented in Table 11 and Table 12. Male respondents may be over-represented (79.4%), but the proportion is not completely out of step with gender ratios found in other IS studies. For example, one study at a large utility in the Eastern United States reported that women comprised 29.4% of the IS development staff (Igbaria & Baroudi, 1995).

Table 11 Personal demographics of respondents

Demographic Variable		Overall		Assoc. 'A'		Assoc. 'B'	
		Count	%	Count	%	Count	%
Gender							
	Male	54	79.4	14	63.6	40	87.0
	Female	14	20.6	8	36.4	6	13.0
	Total	68	100.0	22	100.0	46	100.0
Age							
	Under 20	0	0.0	0	0.0	0	0.0
	20 to 24	0	0.0	0	0.0	0	0.0
	25 to 29	5	7.4	0	0.0	5	10.9
	30 to 34	13	19.1	2	9.1	11	23.9
	35 to 39	7	10.3	0	0.0	7	15.2
	40 to 44	11	16.2	4	18.2	7	15.2
	45 to 49	13	19.1	5	22.7	8	17.4
	50 to 54	12	17.6	4	18.2	8	17.4
	55 to 59	5	7.4	5	22.7	0	0.0
	60 or over	1	1.5	1	4.5	0	0.0
	Missing data	1	1.4	1	4.6	0	0
	Total	68	100.0	22	100.0	46	100.0

Table 12 Educational demographics of respondents

Demographic Variable	Overall		Assoc. 'A'		Assoc. 'B'	
	Count	%	Count	%	Count	%
Education (highest level)						
Some high school	0	0.0	0	0.0	0	0.0
Completed high school	3	4.4	0	0.0	3	6.5
Completed certificate	8	11.8	1	4.5	7	15.2
Some college	4	5.9	2	9.1	2	4.3
Completed college	7	10.3	3	13.6	4	8.7
Some university	13	19.1	5	22.7	8	17.4
Completed university	15	22.1	5	22.7	10	21.7
Some graduate work	4	5.9	1	4.5	3	6.5
Completed graduate work	14	20.6	5	22.7	9	19.6
Other	0	0.0	0	0.0	0	0.0
Total	68	100.0	22	100.0	46	100.0

The median age group was 40 to 44 years, with a range from the 25 to 29 years category, to the 60 years or over category. The sample was bimodal and contains a large number of respondents in the 30 to 34 years category and in the 45 to 49 years category. The recent emergence of security and privacy as a major specialty field within IS may explain the higher than expected frequency in the younger of these two categories. The emphasis on managerial aspects would likely cause practitioners from even younger categories to be less likely (and arguably less qualified, on average) to participate. The large number of respondents in the 45 to 49 years category likely reflects participation from more senior managers, who have found themselves responsible for overseeing IT security efforts.

The educational background of respondents was assessed using ten categories from “Some high school” to “Completed graduate work” (see Table 12). The majority of respondents (approximately two-thirds) reported at least some university education at the undergraduate level or higher. Over 25% of the sample indicated experience at the graduate level. Thus, the sample contains a range of educational backgrounds, with a tendency toward the higher end of the scale.

Demographic results concerning the professional attributes of the participants are presented in Table 13 and Table 14. The average respondent was an employee of the organization he/she considered as his/her primary place of work, had worked there for just under seven years, and spent slightly less than half of that time (M = 3.0 years) in his/her most recent position. The median career position was at a supervisor level with over half of the sample reporting either security/privacy or management as their primary area of expertise. On average, participants reported spending just less than half of their time on IT security matters at work.

While IT security is a significant part of the participants' work concerns, there is diversity in the perspectives reflected in the sample. Additionally, the number of participants reporting a high level of education, substantial work experience, or management level responsibilities indicates that the sample does tap into a population that should be able to respond effectively to questions about managerial topics. It is reasonable to conclude from this data that the respondents, on average, are well qualified to address the types of questions posed in the survey.

Table 13 Professional demographics of respondents

Demographic variable (refers to primary place of work)	Count	%	*M*	*SD*
Tenure at primary place of work			6.8 years	6.9
Tenure in current/most recent position			3.0 years	2.4
Employment type				
Self employed	7	10.3		
Contracting/consulting firm	15	22.1		
Full or part time employee	46	67.6		
Total	68	100.0		
Position type				
Technical	26	38.2		
Supervisor	19	27.9		
Management	12	17.6		
Executive/senior management	10	14.7		
Other	1	1.5		
Total	68	100.0		
Primary area of IS expertise				
Technology	17	25.0		
Applications	7	10.3		
Database	4	5.9		
Security/Privacy	27	39.7		
Management	10	14.7		
Other	2	2.9		
Missing data	1	1.5		
Total	68	100.0		

Table 14 IT security demographics of respondents

Demographic variable (refers to primary place of work)	Count	%	*M*	*SD*
Percentage of time spent on IT security			44.9	38.5
Number of IT security credentials held				
0	44	64.7		
1	17	25.0		
2	5	7.4		
3	2	2.9		
Total	68	100.0		

Comparison of Demographic Data of Participating Associations

Professional demographic data for Association 'A' and Association 'B' are broken out into Table 15 through Table 18, to permit comparisons between the two subgroups. While there are some differences in the intra-group demographics, none of these differences is surprising, given the stated goals of the two associations.

Members of Association 'A' reported slightly longer tenures at their primary places of work and most recent positions. Both groups reported similar employment type and position type characteristics. However, Association 'B' members did show a considerably higher weighting on Security/Privacy as their primary area of expertise. This result is not unexpected, as this group's main focus is security and privacy topics. Similarly, Association 'B' members also reported a higher average amount of time spent on IT security and a higher tendency to hold IT security-related credentials.

Table 15 Professional demographics of Association 'A' respondents

Demographic variable (refers to primary place of work)	Count	%	*M*	*SD*
Tenure at primary place of work			7.7 years	6.8
Tenure in current/most recent position			3.2 years	2.4
Employment type				
Self employed	2	9.1		
Contracting/consulting firm	5	22.7		
Full or part time employee	15	68.2		
Total	22	100.0		
Position type				
Technical	8	36.4		
Supervisor	8	36.4		
Management	3	13.6		
Executive/senior management	3	13.6		
Other	0	0.0		
Total	22	100.0		
Primary area of IS expertise				
Technology	5	22.7		
Applications	6	27.3		
Database	3	13.6		
Security/privacy	3	13.6		
Management	5	22.7		
Other	0	0.0		
Total	22	100.0		

Table 16 IT security demographics of Association 'A' respondents

Demographic variable (refers to primary place of work)	Count	%	*M*	*SD*
Percentage of time spent on IT security			35.5	40.4
Number of IT security credentials held				
0	19	86.4		
1	2	9.1		
2	0	0.0		
3	1	4.5		
Total	22	100.0		

Table 17 Professional demographics of Association 'B' respondents

Demographic variable (refers to primary place of work)	Count	%	*M*	*SD*
Tenure at primary place of work			6.4	7.0
Tenure in current/most recent position			2.9	2.5
Employment type				
Self employed	5	10.9		
Contracting/consulting firm	10	21.7		
Full or part time employee	31	67.4		
Total	46	100.0		
Position type				
Technical	18	39.1		
Supervisor	11	23.9		
Management	9	19.6		
Executive/senior management	7	15.2		
Other	1	2.2		
Total	46	100.0		
Primary area of IS expertise				
Technology	12	26.1		
Applications	1	2.2		
Database	1	2.2		
Security/Privacy	24	52.2		
Management	5	10.9		
Other	2	4.3		
Missing data	1	2.1		
Total	46	100.0		

Table 18 IT security demographics of Association 'B' respondents

Demographic variable (refers to primary place of work)	Count	%	*M*	*SD*
Percent of time spent on IT security			49.3	37.2
Number of IT security credentials held				
0	25	54.3		
1	15	32.6		
2	5	10.9		
3	1	2.2		
Total	46	100.0		

Data Preparation

Missing data

The questionnaire permitted respondents to skip questions, or answer "not sure" if they did not feel able to answer adequately. These instances were dealt with as missing data. Participants not providing valid responses for at least 50% of the items in each of the key constructs (planning, control, organization, integration, and IT security effectiveness) were dropped from further analysis. In the remaining 68 records, there were 26 missing values distributed as shown in Table 19. The total number of values in the key constructs data set, once unusable records were removed, was 1,972 (68 records x 29 observations per record). Thus, the missing values represent only 1.3% of the usable

data set. The item means of valid responses were used to calculate replacement values for missing items, in accordance with the procedure recommended by Hair et al. (1998).

Table 19 Missing data values by construct

Construct/Construct Factor	Count of Missing Data Values
Planning	8
Control	3
Organization	3
Integration	6
IT security effectiveness	6
Total	26

Combining data sets

Due to the size of the sample obtained in this study, it was important to be able to combine the data obtained from both Association 'A' and Association 'B' into one data set for analysis. A MANOVA test was used to compare item response means for the independent and dependent variables of planning, control, organization, integration, and IT security effectiveness. Pillai's Trace criterion, a conservative statistic that is robust under conditions of small sample size and possible unequal cell sizes (Hair et al., 1998), was used to assess the omnibus model. At an alpha level of .05, no significant differences in responses between the two groups were found, $F(5,62) = 0.856$, $p = 0.516$. The data from the two associations were then analyzed as a single data set.

Research Model Analysis

Partial least squares

Analysis of the data was performed using Partial Least Squares (PLS), as implemented in PLS-Graph. This approach to Structured Equation Modeling (SEM) is consistent with that used by the original authors of the IT security effectiveness construct (Kankanhalli et al., 2003). While constructs used in this study were previously validated, the theoretical basis for the study is in the early stages of development. PLS is generally better suited to this type of theory development than other techniques, such as LISREL (Barclay, Higgins, & Thompson, 1995). PLS does not require a specific underlying data distribution or multivariate homogeneity (Chin, 1998). It is also robust in the context of small samples (Barclay et al., 1995). Finally, PLS permits the simultaneous evaluation of both structural and measurement models.

Initial model

The initial (untrimmed) PLS model is presented in Figure 2. All constructs, including the nested model for IS management maturity, were configured using the more conservative mode A (reflective) indicators, as described by Chin (1998). Mode B (formative) maximizes the explained variance of the latent variables (Chin, 1998), and it was felt that this might risk overstating the results. Sample size and multicollinearity within blocks can affect the stability of PLS results, and this difficulty is minimized when reflective mode indicators are used (Chin, 1998). The use of reflective indicators is also consistent with the approach used by Kankanhalli et al. (2003) in that study's analysis of

the IT security effectiveness construct. Finally, for both latent constructs, responses to the perceptual questions in the instrument do not give rise to the constructs, or indicate the presence of precursors to their existence. Rather, responses to the questions reflect perceptions of consequences of the constructs, indicating that a mode A model is appropriate (Barclay et al., 1995).

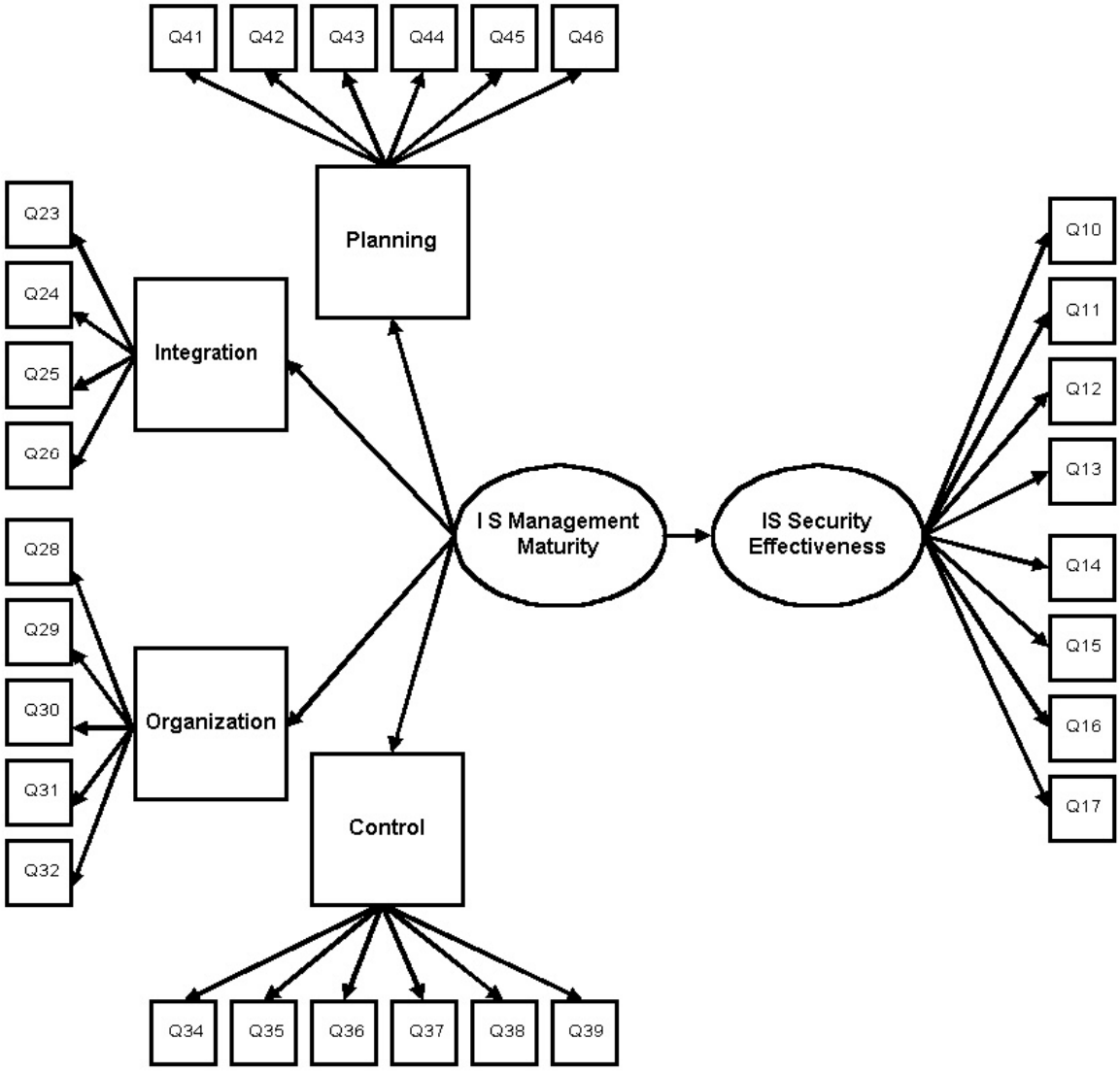


Figure 2. Initial PLS model

The initial factor structures for the independent variable are presented in Table 20, and those for the dependent variable are provided in Table 21. To ensure convergent and discriminant validity, items were examined for adequate loadings on their respective constructs, and low cross-loadings on all others. The generally accepted minimum loading on an intended construct is .707 (Chin, 1998).

Table 20 Initial factor structures (independent variable)

Item	Latent variable for planning	Latent variable for control	Latent variable for organization	Latent variable for integration	Latent variable for security
Planning					
Q41, IT supports business	**.62**	.64	.59	.07	.34
Q42, Examine IT innovation	**.80**	.54	.62	.32	.29
Q43, Inform current IT	**.85**	.43	.58	.40	.29
Q44, Inform potential IT	**.81**	.34	.55	.34	.09
Q45, Org. informed about IT	**.70**	.58	.54	.16	.39
Q46, IT project priorities	**.60**	.42	.55	.22	.11
Control					
Q34, IT direction authority	.56	**.84**	.57	.25	.58
Q35, IT operations authority	.44	**.77**	.57	.18	.49
Q36, IT proposals appraised	.45	**.78**	.43	.11	.40
Q37, IT performance	.56	**.79**	.43	.34	.46
Q38, Clear IT goals	.60	**.86**	.60	.31	.55
Q39, Clear IT performance	.59	**.86**	.48	.31	.48
Organization					
Q28, Ideas of IT personnel	.54	.38	**.76**	.28	.21
Q29, Ideas of end users	.56	.37	**.85**	.26	.24
Q30, IT knows business	.60	.42	**.71**	.10	.47
Q31, IT group structure	.60	.64	**.74**	.19	.50
Q32, End user relations	.65	.60	**.75**	.21	.37
Integration					
Q23, IT is strategic	.36	.32	.39	**.74**	.09
Q24, Top down planning	.34	.46	.37	**.52**	.27
Q25, IT in business units	.17	.13	.03	**.75**	.02
Q26, New IT introduction	.16	.05	.05	**.76**	-.06

For the independent variable, the maturity items were examined for their loadings on the four latent constructs of maturity. Factor loadings for planning, control, organization, and integration are provided in Table 20. Due to poor loadings and cross-loadings, items one and six of the planning construct were dropped from further analysis (Q41, Q46). These items may be flawed, in that they presume the existence of clearly communicated business objectives, strategies, and IT project priorities. This may be a faulty assumption in organizations with low planning sophistication. Without items one and six, item five (Q45) yielded an unacceptable factor loading of .65. Item five of the planning construct was therefore dropped as well, as it appears to tap into control issues of measuring the capabilities and quality of IT systems.

Table 21 Initial factor structures (dependent variable)

Item	Latent variable for planning	Latent variable for control	Latent variable for organization	Latent variable for integration	Latent variable for security
Q10, Security of hardware	.31	.55	.33	.02	**.83**
Q11, Security of software	.28	.53	.33	.00	**.86**
Q12, Security of data	.30	.56	.41	.04	**.91**
Q13, Security of services	.22	.46	.44	-.01	**.85**
Q14, Deter insiders	.27	.51	.34	.08	**.78**
Q15, Prevent insiders	.37	.43	.44	.26	**.73**
Q16, Deter outsiders	.17	.44	.34	.06	**.76**
Q17, Prevent outsiders	.28	.45	.39	.18	**.80**

Item two of the integration construct (Q24) loaded poorly in the context of the other three items. When this item was removed, problems were encountered with the stability of the construct. No stable configuration of the items could be created using PLS, possibly due to bi-dimensionality. Items one and two of the integration construct (Q23, Q24) seem to be more closely related to planning or management support for IS. Items three and four may simply be unreliable, as they were also removed in another study that used this construct (Karimi et al., 2000). As a result, the integration construct was removed from further analysis.

For the dependent variable, initial factor structures are presented in Table 21. All items loaded well onto the security effectiveness latent construct, with values well over the minimum of 0.707. No problematic cross-loadings were found. All eight items of IT security effectiveness were kept.

Trimmed model

The trimmed PLS model is presented in Figure 3 and the trimmed factor structures are shown in Table 22. All items can be seen to load adequately on their intended factors, with comparatively low cross-loadings. This trimmed model was used for all further analysis.

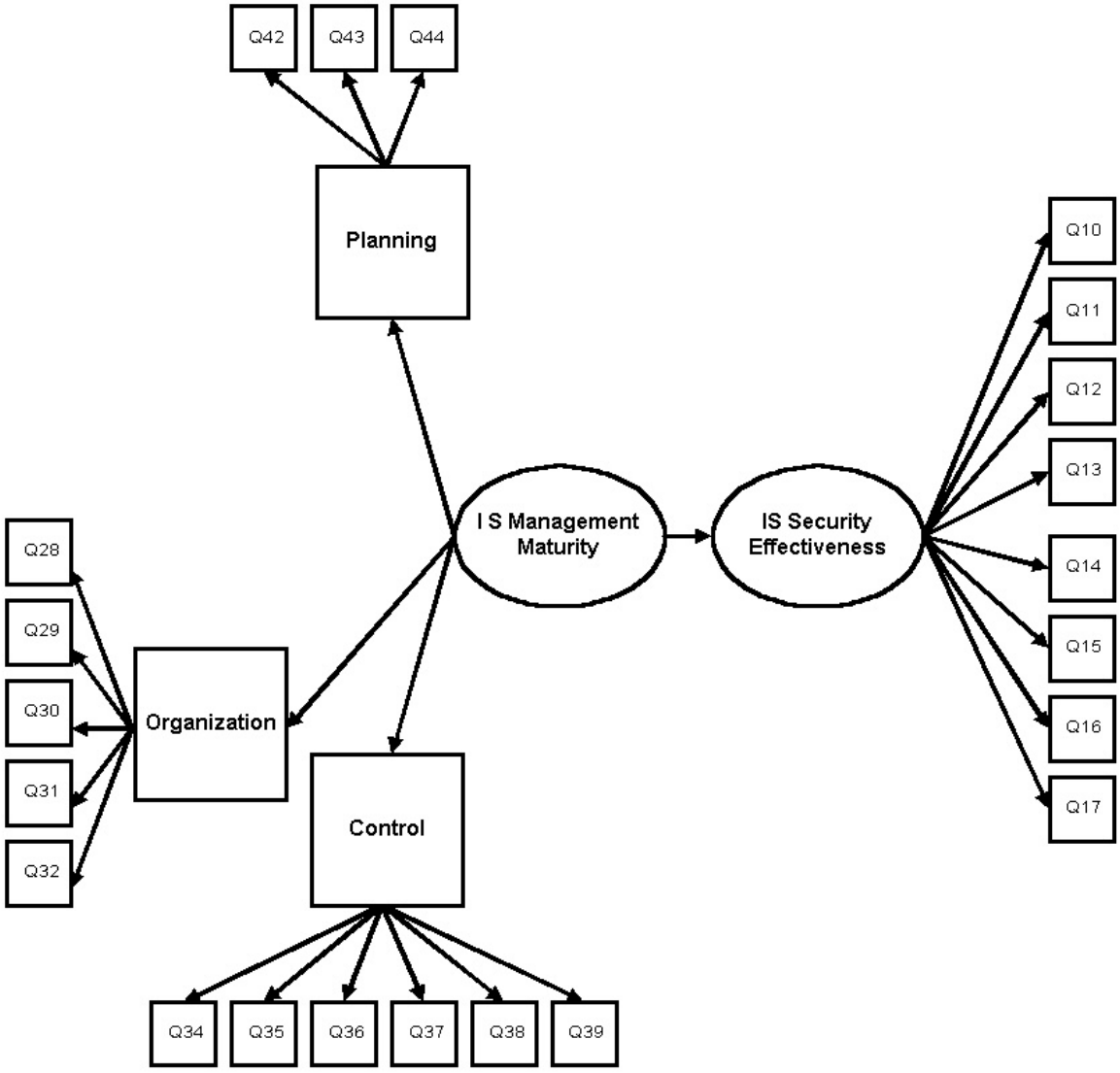


Figure 3. Trimmed PLS model

Table 22 Trimmed factor structures

Item	Latent variable for planning	Latent variable for control	Latent variable for organization	Latent variable for security
Planning				
Q42, Examine IT innovation	**.83**	.54	.62	.29
Q43, Inform current IT	**.92**	.43	.58	.29
Q44, Inform potential IT	**.91**	.34	.55	.09
Control				
Q34, IT direction authority	.45	**.84**	.57	.58
Q35, IT operations authority	.27	**.77**	.57	.49
Q36, IT proposals appraised	.27	**.78**	.43	.40
Q37, IT performance	.43	**.79**	.43	.46
Q38, Clear IT goals	.49	**.86**	.60	.55
Q39, Clear IT performance	.48	**.86**	.48	.48
Organization				
Q28, Ideas of IT personnel	.49	.38	**.76**	.21
Q29, Ideas of end users	.50	.37	**.85**	.24
Q30, IT knows business	.49	.42	**.71**	.47
Q31, IT group structure	.48	.64	**.74**	.50
Q32, End user relations	.56	.60	**.75**	.37
Security effectiveness				
Q10, Security of hardware	.23	.55	.33	**.83**
Q11, Security of software	.17	.53	.33	**.86**
Q12, Security of data	.20	.56	.41	**.91**
Q13, Security of services	.09	.46	.44	**.85**
Q14, Deter insiders	.23	.51	.34	**.78**
Q15, Prevent insiders	.35	.43	.44	**.73**
Q16, Deter outsiders	.14	.44	.34	**.76**
Q17, Prevent outsiders	.25	.45	.39	**.80**

Descriptive statistics

Descriptive statistics for all items retained in the trimmed model are presented in Table 23. The 22 retained items in the trimmed model were all implemented using a five-point Likert scale ranging from 1 (*strongly disagree*) to 5 (*strongly agree*). The means range from 3.23 (Q44) to 4.03 (Q17). The standard deviations range from 0.83 (Q43 and Q28) to 1.25 (Q14). Floor effects in these results therefore seem unlikely. Ceiling effects do not seem to pose a significant problem either, although some of the items related to IT security effectiveness do show high mean values and large standard deviations that approach the top end of the measurement (Q10, Q12, and Q17).

Descriptive statistics for the combined item scores of each of the constructs are presented in Table 24. On average, respondents agreed somewhat with the IS management maturity survey statements for planning (M = 3.37), control (M = 3.47), and organization questions (M = 3.69). The overall average for all IS management maturity items[5] (M = 3.53) indicates that the participants agreed somewhat with the IS management maturity questions, as a whole. However, more than 20% of participants disagreed with questions 34 (IT direction authority, 26.5%), 37 (IT performance, 20.6%), 39 (Clear IT performance, 20.6%), 44 (Inform potential IT, 22.1%), and 46 (IT project priorities, 20.6%)[6]. Three of these were control questions (Q34, Q37, and Q39) and two were planning questions (Q44 and Q46), suggesting that some of the respondents see weaknesses in these aspects of IS management.

[5] The overall average for IS management maturity items is an unweighted mean of the means of the three retained IS management maturity measures (planning, control, and organization).
[6] Due to space limitation the frequencies of the various items have not been included, but can be obtained from the author.

Table 23 Descriptive statistics of trimmed model items

Item	*M*	*SD*
Planning		
Q42, Examine IT innovation	3.45	1.01
Q43, Inform current IT	3.42	0.83
Q44, Inform potential IT	3.23	0.88
Control		
Q34, IT direction authority	3.40	1.01
Q35, IT operations authority	3.75	0.97
Q36, IT proposals appraised	3.30	0.93
Q37, IT performance	3.52	0.97
Q38, Clear IT goals	3.57	0.95
Q39, Clear IT performance	3.31	1.00
Organization		
Q28, Ideas of IT personnel	3.75	0.83
Q29, Ideas of end users	3.64	0.87
Q30, IT knows business	3.60	0.90
Q31, IT group structure	3.62	0.96
Q32, End user relations	3.84	0.84
IT security effectiveness		
Q10, Security of hardware	3.91	1.02
Q11, Security of software	3.65	1.09
Q12, Security of data	3.69	1.07
Q13, Security of services	3.76	1.05
Q14, Deter insiders	3.47	1.25
Q15, Prevent insiders	3.90	0.98
Q16, Deter outsiders	3.39	1.15
Q17, Prevent outsiders	4.03	0.90

Note. All items were scored on a five-point Likert scale ranging from 1 (*strongly disagree*) to 5 (*strongly agree*).

Table 24 Descriptive statistics of combined item scores (trimmed model)

Construct	*M*	*SD*
Planning	3.37	0.91
Control	3.47	0.98
Organization	3.69	0.88
IS management maturity	3.53	0.94
IT security effectiveness	3.72	1.08

Note. All items were scored on a five-point Likert scale ranging from 1 (*strongly disagree*) to 5 (*strongly agree*).

Practitioners were also in agreement, on average, with the IT security effectiveness questions (see Table 23). The lowest average response was for the item measuring perceived effectiveness of preventing attacks by insiders ($M = 3.39$). The highest average response was for the item measuring perceived effectiveness of preventing attacks by outsiders ($M = 4.03$). The overall mean response for IT security effectiveness items ($M = 3.72$) indicates that respondents, on average, agreed with the IT security effectiveness questions in the context of their respective organizations (see Table 24). However, more than 20% of participants disagreed with questions 14 (Deter insiders, 23.5%), and 15 (Prevent insiders, 28%), suggesting that some of these practitioners see weaknesses in these aspects of IT security.

Analysis and interpretation of PLS model

The following presents the analysis and interpretation of the PLS model. Barclay et al. (1995, p. 295) suggests performing this in two stages. First, the measurement

model is evaluated for reliability and validity. Then, the structural model is evaluated for significance and substantiveness.

The measurement model assesses the association between each construct and the items used to measure it. To perform this analysis, Barclay et al. (1995) recommends examining the reliability of individual items, internal consistency, and discriminant validity.

The factor scores of the individual items are shown in Table 22. Loadings are correlations (Barclay et al., 1995), and should therefore exceed .707 on the intended construct, as an indication of less than 50% ($.707^2 = .499$) unexplained variance (i.e. noise component) in the item. Convergent validity is thus demonstrated by each item sharing greater than 50% of its variance with the intended construct. All of the retained measures in the trimmed model clearly met this criterion. Loadings for the nested model are presented in Table 25. Again, it is clear that the nested latent variables and items retained in the trimmed model load well onto the intended constructs.

Internal consistency and convergent validity are assessed here using the Fornell and Larcker (1981) equation, and Average Variance Extracted (AVE), respectively. The Fornell and Larcker measurement is similar to the more commonly used Cronbach's Alpha and is interpreted in much the same manner, so the accepted minimum for this measure is .70 (Barclay et al., 1995). However, the Fornell and Larcker calculation is considered superior and is more widely accepted amongst researchers using PLS (Barclay et al., 1995). Both of the key constructs (IS management maturity and IT security effectiveness) and the lower order model constructs for IS management maturity

(planning, control, and organization) exceeded the cutoff for internal consistency, as shown in Table 26.

Table 25 Factor loadings of nested model

Latent variable or item	Latent variable for IS management maturity	Latent variable for IT security effectiveness
Latent variable for planning	**0.75**	0.25
Latent variable for control	**0.89**	0.60
Latent variable for organization	**0.89**	0.46
Q10, Security of hardware	0.48	**0.83**
Q11, Security of software	0.46	**0.86**
Q12, Security of data	0.51	**0.91**
Q13, Security of services	0.44	**0.85**
Q14, Deter insiders	0.46	**0.78**
Q15, Prevent insiders	0.48	**0.73**
Q16, Deter outsiders	0.40	**0.76**
Q17, Prevent outsiders	0.45	**0.80**

AVE gauges the shared variance of a construct and the items used to measure it (Barclay et al., 1995), as compared to the variance due to measurement error (Chin, 1998). Essentially, this is the degree to which the construct items tap into the same underlying construct (Kankanhalli et al., 2003). AVE should exceed .50, indicating that at least 50% of the variance of the indicators can be explained (Chin, 1998). The results presented in Table 26 indicate an adequate level of convergent validity in the two key

constructs (IS management maturity and IT security effectiveness) and the lower order model constructs for IS management maturity (planning, control, and organization).

Table 26 Internal consistency and convergent validity of constructs

Construct	Internal consistency[7]	Average Variance Extracted[8]
Planning	.92	.78
Control	.92	.67
Organization	.87	.58
IS management maturity	.88	.71
IT security effectiveness	.94	.67

Discriminant validity, the extent to which measures of a construct maintain low correlations with other constructs, is an indication of the uniqueness of a construct (Barclay et al., 1995). Chin (1998), states that an indication of acceptable discriminant validity is when the square root of AVE exceeds the correlations between constructs. As is shown in Table 27, the nested model used here meets this criterion.

[7] Fornell and Larcker's measure of internal consistency is (Barclay et al., 1995, p. 306):

$$\frac{\left(\sum \lambda_{yi}\right)^2}{\left(\sum \lambda_{yi}\right)^2 + \sum Var(\varepsilon_i)}$$

where λ_{yi} is the component loading and $Var(\varepsilon_i) = 1 - \lambda_{yi}^2$

[8] The formula for Average Variance Extracted (AVE) is (Barclay et al., 1995, p. 306):

$$\frac{\sum \lambda_{yi}^2}{\sum \lambda_{yi}^2 + \sum Var(\varepsilon_i)}$$

where λ_{yi} is the component loading and $Var(\varepsilon_i) = 1 - \lambda_{yi}^2$

A second condition for acceptable discriminant validity is to have all items load highest on the construct they are intended to measure (Barclay et al., 1995). Since any items that cross-loaded too strongly were removed in the trimmed model, this criterion is satisfied. (Table 22 provides the trimmed factor structures.) Additionally, the latent variables within the nested model also fulfill this discriminant validity condition, as presented in Table 25.

Table 27 Discriminant validity of constructs

Construct	IS management maturity	IT security effectiveness
IS management maturity	**.85**	
IT security effectiveness	.57	**.82**

Note. Diagonal elements in bold are square roots of AVE. The off-diagonal element is the correlation between the constructs.

Once the validity and reliability of the measurement model were confirmed, analysis of the structural model was undertaken to assess the relation between the constructs. Evaluation of the structural model was performed by examining the predictive power of the model, as well as the path coefficient and its statistical significance. A summary of the results is presented in Table 28 and the structural model results are shown in Figure 4.

Table 28 Structural model results

Path	Standardized path coefficient	t-Value for path
H1: IS management maturity --> IT security effectiveness	.57	7.69***

Note. *** $p < .001$
R^2 for IT security Effectiveness = .32

The structural model was able to account for 32% of the variance in the endogenous construct (see Figure 4). The jackknifing procedure (Chin, 1998) was used to calculate the t-statistic for the path coefficient. IS management maturity was positively associated with IT security effectiveness, $t = 7.69$, $p < .001$. H1 was supported.

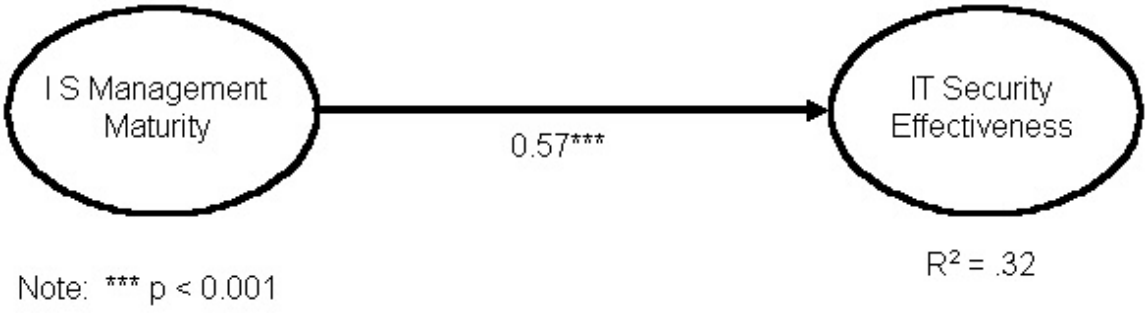


Figure 4. PLS structural model results

Barclay et al. (1995) suggests that any model with greater than 25% explained variance has merit. The original authors of the IT security effectiveness construct used here (Kankanhalli et al., 2003) note that others have suggested a 10% cutoff for establishing substantive explanatory power. In either case, the results obtained in this study clearly meet the suggested criterion.

Comparing the results obtained in this study to others that used similar constructs, or examined issues in the same general research area, can also provide insights to the substantiveness of this study's findings. Kankanhalli et al. (2003) reported that the model used in that study was able to explain 18.7% of the variance in IT security effectiveness. The study used three independent variables (organizational size, top management support, and industry type) and three mediating variables (deterrent efforts, deterrent severity, and preventive efforts) to predict IT security effectiveness. An earlier study by Goodhue and Straub (1991) achieved 5% explained variance by using industry risk, company actions, and individual awareness to predict the security concern level of end users. Finally, a third study (Straub, 1990b) used IT security deterrents and preventive measures to predict rates of system abuse, and reported explained variance levels between 24.2% and 37.4%.

These comparative results suggest that the explanatory power of this study's model is substantive and that the perceived maturity of an organization's IS management practices positively correlates with the perceived effectiveness of its IT security safeguards.

Discussion and Conclusions

This study examined the relation between IS practitioners' perceptions of IS management maturity and their perceptions of IT security effectiveness. IS management maturity, an expression of the sophistication of an organization's IS management practices, was assessed with perceptual measures for planning, control, organization, and integration, based on prior work by Karimi et al. (1996). IT security effectiveness was assessed with measurements for the perceived effectiveness of protection provided by safeguards for hardware, software, data, and services as well as overall deterrent and preventive effects. The IT security measures were based on prior work by Kankanhalli et al. (2003).

A cross-sectional web-based survey of English-speaking IS practitioners in Canada was performed. The sample frame consisted of IS practitioners who were members of two selected Canadian IS associations at the time of the study. The number of usable responses was lower than anticipated (N = 68), but this was still adequate for analysis using Partial Least Squares (PLS).

Findings

This study's findings show a positive correlation between the participants' perceptions of IS management maturity (the exogenous construct) and their perceptions of IT security effectiveness (the endogenous construct). The path coefficient of the PLS structural model (.57) was shown to be statistically significant ($t = 7.69$, $p < .001$) and the structural model was able to account for 32% of the variance in the endogenous construct. Barclay et al. (1995) suggests that any PLS model with greater than 25%

explained variance has merit. Overall the hypothesis that perceived maturity in IS management practices is positively associated with perceived IT security effectiveness was supported (path coefficient = .57).

IT security effectiveness

The mean response overall for IT security effectiveness items (M = 3.72) implies agreement with the survey questions (see Table 24). That is, on average, respondents indicated that they viewed IT security safeguards within their organizations as effective. Furthermore, the results show a consistency in this perception across the different types of IT assets. From the highest of these means, for security of hardware (M = 3.91), to the lowest, security of software (M = 3.65), the average responses were consistently in agreement with the survey questions (see Table 23). The mean responses varied slightly more for the items pertaining to the effectiveness of different safeguard classes. Nonetheless, from the highest of these, effectiveness of preventive measures against outsiders (M = 4.03), to the lowest, effectiveness of preventive measures against insiders (M = 3.39), respondents still agreed, on average, with the survey questions. Thus, on the whole, these respondents indicated a perception of effectiveness in IT security safeguards.

However, it is worth noting that more than 20% of participants disagreed with questions 14 (Deter insiders, 23.5%), and 15 (Prevent insiders, 28%), suggesting that some of these practitioners see weaknesses in these aspects of IT security. Preventing violations by insiders can be problematic. Dishonest insiders may have legitimate access to the IS assets of concern (Courtney, 1977), and may therefore be aware of potential

vulnerabilities in existing security mechanisms. Insiders are also more likely to engage in abusive behaviour (Hoffer & Straub, 1989).

The fact that the practitioners who took part in this survey seem to be indicating that they believe IT security safeguards are, on average, effective, seems to contradict other recent surveys (Power, 2002; Richardson, 2003). It is possible that Canadian practitioners perceive a lower threat level than is perceived in other geographic areas. A recent study, co-sponsored by the Royal Canadian Mounted Police, noted that few Canadian corporate executives "see their organizations as being at significant risk of attack" (Kapica, 2003). A lower perceived threat level could have the effect of causing IT security safeguards to appear more effective, on average, in a Canadian context. Alternatively, reporting on the problem may be flawed. As an example, a recent poll asked CEOs from mid-size Canadian companies to rate the effectiveness of IT security safeguards within their organizations, using a three-point scale of *very effective*, *somewhat effective* or *somewhat ineffective* (Ferneyhough, 2002). The poll somewhat alarmingly reported that only 30% of the CEOs considered IT security safeguards to be "very effective" (Ferneyhough, 2002, p. 2). However, this statement may be misleading. An examination of the detailed tables shows that almost two thirds (approximately 62%) of the respondents considered IT security safeguards to be "somewhat effective" (Ferneyhough, 2002). So, the finding that the majority of that poll's respondents (approximately 92%) perceived at least some effectiveness in their existing IT security safeguards seems to be more in line with this study's findings.

IS management maturity

Results for IS management maturity echoed those for IT security. The overall mean for all maturity items (M = 3.53) implies that the respondents agreed somewhat with the survey questions. Thus, the participants seem to perceive an adequate level of IS management maturity in their organizations. As with the IT security effectiveness measurements, there is consistency in these results. The mean responses for planning (M = 3.37), control (M = 3.47), and organization (M = 3.69) all demonstrate agreement with the survey questions. The following sections discuss ways in which the components of IS management maturity (planning, control, organization, and integration) may contribute to the effectiveness of IT security.

Planning

This component is concerned with alignment of IT with the business and use of managerial planning for improving the use of IT throughout the organization (Karimi et al., 1996). See Table 7 for a comparison of the original questions used by Karimi et al. (1996), and the adapted questions used in this study. Items one and six of the planning construct (Appendix A, Q41, Q46) were dropped from analysis. These items seem to presume the existence of clearly communicated business objectives, strategies, and IT project priorities, which may be a faulty assumption, especially in organizations with low planning sophistication. Item five (Appendix A, Q45) of the planning construct appears to tap into control issues concerning measurement of the capabilities and quality of IT systems, and was also removed. The remaining items were found to be valid and reliable

in the context of IS security, which is a new context from that in which these measures were originally developed by Karimi et al. (1996).

While respondents, on average, agreed with the survey questions for planning (*M* = 3.37), more than 20% of participants disagreed with questions 44 (Inform potential IT, 22.1%), and 46 (IT project priorities, 20.6%). This suggests that some participants see weaknesses in their respective organizations' practices concerning planning for future use of IT, and setting priorities for IT projects.

It can be argued that many short-term security efforts are reactions to failures in longer-term planning activities. For example, the need to investigate a security incident may be due to a breakdown in safeguards that should have been designed to prevent the problem. Maturity in IS planning practices would therefore seem to be likely to benefit IT security.

Control

This component is concerned with the use of a managerial orientation toward measuring IT value, basing controls on benefits, priorities, and standards (Karimi et al., 1996). See Table 8 for a comparison of the original questions used by Karimi et al. (1996), and the adapted questions used in this study. All of the control maturity items were found to be valid and reliable in the context of IS security.

While respondents, on average, agreed with the survey questions for control (*M* = 3.47), more than 20% of participants disagreed with questions 34 (IT direction authority, 26.5%), 37 (IT performance, 20.6%), and 39 (Clear IT performance, 20.6%). This suggests that some participants see weaknesses in their respective organizations' control

practices concerning assignment of overall authority and responsibility for IT, regular monitoring of IT performance, and clear performance criteria for the IT group.

Security has traditionally been implemented using control mode approaches based on policies, guidelines, standards, and practices. Auditors, historically a part of organizational management control structures, have, with varying degrees of success, made extensive use of policies and guidelines as frameworks to substantiate their opinions on IT security as an internal control matter (*COBIT: Control objectives*, 2000). IT security safeguards are sometimes even referred to as "controls" (*COBIT: Control objectives*, 2000; *ISO/IEC 17799:2000*, 2000). The connotation is that safeguards provide management with a means of controlling the use of IS by monitoring its use and restricting the functionality of the related systems and services. Recent work continues to emphasize the use of control mode management techniques for IT security, such as improvements in security metrics (Christie & Goldman, 2003). It follows that organizations with mature managerial practices for control of overall IS functions are likely well prepared to implement effective control measures related to IT security.

Organization

This component of maturity concerns the roles and responsibilities of users and IT personnel, and the level in the organization at which IT management resides. See Table 9 for a comparison of the original questions used by Karimi et al. (1996), and the adapted questions used in this study. All of the control maturity items were found to be valid and reliable in the context of IS security.

Respondents, on average, agreed with the survey questions for control (M = 3.69). Furthermore, there were no items with which more than 20% of participants disagreed. This suggests that participants did not perceive areas of particular weakness in the organization practices of their respective organizations.

The need to address organizational factors is emphasized in IT security practice literatures. For example, in a recent article the authors note the need to consider "complex organizational dynamics, such as vertical industry, operational models, company location, user distribution, and corporate financial health" (Briney & Prince, 2002, p.36) as key factors in IT security decision-making processes. The international standard *Code of Practice for Information Security Management* (*ISO/IEC 17799:2000*, 2000) dedicates an entire chapter to organizational security, emphasizing the need for specifying roles, responsibilities, information flows, and organizational entities. It would seem to follow that more mature IS organization structures are not only better suited to supporting general organizational requirements, but are also more likely to have success implementing and maintaining effective security practices.

Integration

Integration refers to the use of top down planning for IT, increased technology transfer, and greater exploitation of technology throughout the firm (Karimi et al., 1996). The items used to assess IS integration (Appendix A, Q23, Q24, Q25, Q26), although based on previous research (Karimi et al., 1996), had to be removed from the analysis due to stability problems in the measurement. No combination of two or more items from this study's data produced a usable result. In later research using this construct, Karimi et

al. (2000) removed two of the four integration items that related to experimentation with, or development of, IT capabilities at the business unit level (equivalent to Appendix A, Q25, Q26). These items may simply be unreliable. The other two items (Appendix A, Q23, Q24) concern the perception of IT as a strategic resource and the presence of a top-down planning process for IT. On post hoc examination, these items appear to be tapping into a construct that might be better identified as managerial support or advocacy for IS, as implemented by other researchers (Aladwani, 2002; Igbaria & Baroudi, 1995; Yoon, Guimaraes, & O'Neal, 1995). Further work appears to be necessary to develop a more robust measurement for this dimension of IS management maturity.

Conclusions

Using previously validated measurements for IS management maturity (Karimi et al., 1996) and IT security effectiveness (Kankanhalli et al., 2003), this study found a strong, positive correlation between the participants' perceptions of IS management maturity and IT security effectiveness. Thus, this study provides evidence that organizational factors in addition to those examined by Kankanhalli (2003) may influence the effectiveness of IT security safeguards. IS practitioners, the participants in this study, are likely to be informed about, and influential concerning, both IS management and IT security. As such, their perspectives on these subjects are useful (Goodhue & Straub, 1991), and are believed to generally reflect practices in place within their respective organizations.

This study did not address how IS management maturity might relate to the organizational and mediating variables of the integrative model used by Kankanhalli et al. (2003). Further investigation would therefore be required to assess how this study's findings might be used to augment those of Kankanhalli et al. (2003). However, the results of this study do imply that the organizational variable, IS management maturity, may also be a positive contributor to the effectiveness of an organization's IT security efforts.

As an organization's IS practices mature, the additional attention paid to IS by management may contribute to improvements in the organization's ability to cope with the complexities of IT security. Also, mature IS management practices may be more likely to allocate the necessary resources to meet the demanding nature of effective IT safeguarding. While the methodology used in this study cannot demonstrate causation, it seems possible that the organizational changes associated with increased IS management maturity are beneficial to the effectiveness of IT security efforts. Specifically, increasing levels of sophistication in IS management planning, control, and organization activities may play an important role in improving IT security safeguarding.

Contributions

This study is one of the first to examine IS management maturity in the context of IT security and found a strong, positive correlation between the participants' perceptions of IS management maturity and IT security effectiveness. The notion of maturity has been applied to security in other ways (Siponen, 2002; Stacey, 1996; *SSE-CMM*, 2003). Previous studies have also examined specific managerial variables in the context of IT

security, including top management support (Kankanhalli et al., 2003), MIS executive concerns (Loch et al., 1992), disciplinary response to computer abuse (Straub, 1990a, 1990b), and allocation of organizational resources (Goodhue & Straub, 1991; Straub, 1990b). No prior research has been found that empirically tested a model of IS management maturity in the context of IT security. This study has therefore provided a new and useful perspective on the matter of protecting IT assets.

A complex, multi-dimensional construct was used to measure perceived IS management maturity, avoiding problems inherent in the use of simpler models. The management maturity measurements developed by Karimi et al. (1996) generally held in the new context of IS security, but this study did encounter problems applying some of the measures for integration and planning maturity. The original authors of these measurements (Karimi et al., 1996) experienced similar difficulties (Karimi et al., 2000), suggesting that additional work is required to produce stable items. The study described here also successfully refined the items originally used by Karimi et al. (1996) (see Table 7 to Table 10), and added an item to the organization component of IS maturity (the influence of IT personnel on IT planning and implementation, see Appendix A, Q28).

This investigation successfully refined the IT security effectiveness measurement introduced by Kankanhalli et al. (2003). Use of the insider/outsider dichotomy for the deterrent and preventive measures provided additional insight into how practitioners perceive the effectiveness of these approaches in different threat contexts. These refinements can be of significant value to practitioners and researchers in understanding the effect of different safeguarding modes, and in the development of security plans or architectures.

Finally, this study provides further information in a very under-researched area. As noted by Dhillon (2003), there is both a lack of research into IT security and an acute need for better understanding of IT security matters, due to threats from both insiders and outsiders. The strong relation found here between perceived IS management maturity and perceived IT security effectiveness provides a clear indication of an important part of successful IT safeguarding. Furthermore, the design of this study permitted an investigation of various aspects of both security and maturity, providing valuable insights into factors that help to explain effectiveness of security in IT. Ultimately, the results of this study yield an important perspective on how IS practitioners perceive the influence that management can have on the protection of valuable organizational resources.

Limitations of This Study

The primary limitation of this study is the low response rate. IS practitioners are a difficult population to access in Canada, since the profession is not regulated nationally or in any province. Consequently, there is no simple means of identifying, enumerating, assessing, or contacting this population, as a whole. This made it impractical to ascertain the extent to which the professional associations that comprised the sample frame in this study actually reflect the broader population. Nonetheless, the associations that participated in this study are felt to have been the best sample frame available at the time.

Because there was no means of directly contacting potential participants, there exists the possibility of a self-selection bias amongst respondents to the solicitation notices. Moreover, the low response rate by Association 'A' raises some concern about the degree to which the sample is representative of the sample frame. However, the

demographics of the respondents indicate that they were appropriate for the study, and that a range of perspectives is reflected in the data. Additionally, the strong results and reasonable item variances (see Table 23) demonstrate that coherent responses were acquired from this sample. Although variance was probably lost with the small sample size, the relationship between IS management maturity and IT security effectiveness was significant. While caution is appropriate in the interpretation of these results, they are consistent with both theory and practice and do not present any serious explanatory difficulties.

Additional limitations of this research include the use of a very new measurement for IT security effectiveness, the application of maturity in a new context, and the lack of a causal explanation for the findings. Strong factor loadings and high reliability were achieved with the IT security effectiveness measurement, and the results are consistent with those reported by Kankanhalli et al. (2003). This alleviates much of the concern related to the use of this new measurement. Similarly, the results achieved with the IS management maturity construct suggest that the measurement was used successfully in the new context of IT security. The parallel difficulties with the integration and planning constructs reported here and by Karimi et al. (2000), further imply that this measurement was suitably implemented in this study. Finally, it is a limitation of the research methodology that causality cannot be conclusively determined. This is therefore left as an avenue for future research.

In view of the limitations just mentioned, there are constraints on this study's external validity. That is, the sample obtained in this study's survey may not be representative of the population of IS practitioners. For example, this study's survey may

have tended to attract more highly motivated respondents, who may, in turn, tend to reflect more mature organizations. Additionally, the IS practitioner associations used in this study's sample frame may tend to attract a non-representative subset of the population of IS practitioners. Accordingly, care should be used when generalizing these results to the entire population of IS practitioners. But, this research maintains its usefulness for academics, in the development of further research hypotheses, and for practitioners, as a model for adaptation to specific situations.

Finally, the survey was designed to be simple and easy to complete for respondents. There exists the possibility that this may have introduced a methods bias that influenced respondents to over or under state their true perceptions. Additionally, it is possible that participants may have simply attempted to provide consistent responses throughout the survey, causing a response bias. Such biases may reduce the internal validity of the results obtained in this study. Additionally, measuring the perceptions of IS practitioners, rather than alternatives, such as rates of security abuse (Goodhue & Straub, 1991), may have introduced perceptual biases into the data. Nonetheless, these perceptual measurements have been used before by other researchers (Kankanhalli et al., 2003; Karimi et al., 1996) who validated their psychometric properties and reported similar results to those obtained in this study.

Directions for Future Research

Clearly, the first direction that future research in this area should take is to replicate this study with additional samples. In other geographic areas it may be practical to establish better sample frames. Also, practitioners from other regions may indicate a

different level of concern for the effectiveness of IT security safeguards. Beyond this, further work could seek to understand how the different components of maturity relate to security effectiveness or examine in detail the mechanisms that underlie how improvements in maturity can influence IT security. Experimental research could facilitate an understanding of the causal links underlying this study's findings. Alternatively, a longitudinal analysis of the variables used in this study would shed some light on which components of maturity may be of greater or lesser interest at different points in the evolution of an organization's IS management practices.

Despite the substantive explained variance achieved in this study (see Table 28, Figure 4) other variables must also be influential in terms of an organization's IT security effectiveness. Organizational culture and reliance on IS are suggested by Kankanhalli et al. (2003), along with various deterrent and preventive measures. Research that extended the analysis beyond deterrent and preventive measures, to include detection[9], containment, and recovery protection classes (see Table 2) would provide a more useful set of security capability design options for practitioners. The possibility of preconditions, such as the legal environment or social norms may also be of important predictive value.

More work is needed to develop an IS management maturity measurement that is robust in the context of IT security. Considering the experience of this study, and that of Karimi et al. (2000), improvements in the integration measures should be the first priority, followed by a refinement of the items used to measure planning. Progress in these areas would likely improve the predictive value of this study's model and permit

[9] Detection is specifically mentioned by Straub (1986b) as an avenue for extending this analysis.

future investigations to examine possible relations between integration maturity and security effectiveness.

Implications for Practice

In general, as systems increase in technical complexity, corresponding improvements in management techniques are required (Drury, 1983). The results obtained in this study suggest that there is a positive association between IS practitioners' perceptions of an organization's IS management maturity level, and the organization's capacity to deal with the complexities of IT security. Practitioners should therefore consider how this might affect the selection of IT security safeguards. The implementation of advanced security technologies, for instance, may be of limited value if the organization cannot adequately manage its existing systems. One author states that IS managers who install Intrusion Detection Systems (IDS) may not obtain the level of protection they are seeking if they do not already have a thorough understanding of the organization's current systems (McQuillan, 2002). This problem may be exacerbated if managers or end users refuse to accept new safeguards because they are, or appear to be, too sophisticated to be meaningful within the organizational setting (Dhillon & Backhouse, 1996). In these situations, security practitioners might do better to concentrate on improving management processes for existing systems, rather than acquiring additional, complex equipment. This is not to say that appropriate security tools are not necessary, only that the organization must be prepared to adapt to the complexities of each tool it adopts. As an organization's IS management practices increase in sophistication, more complex IT security safeguards may become likely to

provide effective protection. Organizations would therefore do well to consider the maturity of their management practices when selecting IT security safeguards.

An important distinction should be made at this point. This study is not suggesting that practitioners should attempt to make their organizations more mature through some artificial technique, nor is it suggesting that becoming mature in IS management will somehow result in immediate improvements in IT security. The processes that underlie changes in an organization's IS management sophistication level are complex, and beyond the scope of this study. Rather, the implication here is that practitioners should consider the sophistication of the IS management practices in an organization as part of the safeguard selection process.

IT security practitioners also need to become more involved at the management level, integrating security considerations into improvements in overall IS management. While security practitioners may already be comfortable contributing to control aspects of IS management, they should also consider increasing their involvement in IS planning and organization activities. As shown by Karimi et al. (2000), different types of steering committees (e.g., steering groups and policy committees) can positively influence various aspects of IS management maturity (e.g., planning and organization). Security practitioners should consider participation in such committees where possible. Additionally, Gupta et al. (1997) demonstrates that organizations with different strategic orientations tend to emphasize different aspects of IS maturity. Security practitioners should make use of increased involvement at the managerial level to consider these issues when examining the links between IS management practices and IT security.

Reasons for different IS management sophistication levels within organizations are beyond the scope of this paper, but are discussed widely in the IS academic literature. Competitive strategy (Gupta et al., 1997), age of specific IS functions (e.g. security) within the organization (Straub, 1990b), resource allocation (Karimi et al., 2000), external forces such as technological change and advancements in knowledge (King & Kraemer, 1984), and IS education or experience of top management (Karimi et al., 2001) may all be related to the maturity of IS management practices. Other possibilities include organization size and stability, industry type, level of competition, and regulatory environment. It seems likely that these factors may, in turn, influence an organization's investment level in IT security. However, it is often impractical for IS practitioners to directly affect many of these variables. Therefore, IS practitioners should focus their efforts on ensuring a good match between the complexity of IT security safeguards and the IS management maturity level of the organization, taking into account the likelihood of growth and change.

Finally, over 20% of participants disagreed with the survey questions regarding overall preventive and deterrent effects of IT security safeguards in the context of insider threats (Appendix A, Q14, Q15). Thus, while the overall perception was that security safeguards are effective, a substantial number of respondents saw weaknesses in aspects of IT security related to protecting against insiders. Practitioners may therefore want to focus additional effort on safeguards that address internal threats, such as stronger policies, more rigorous enforcement of those policies, and better access control procedures.

Summary

This project empirically evaluated a model of the relation between IS practitioners' perceptions of IS management maturity and their perceptions of IT security effectiveness. Specifically, the perceived maturity of management practices related to IS planning, control, organization, and integration were tested for their association with the perceived effectiveness of security safeguards for IS hardware, software, data, and services, and for the overall perceived effect of deterrent and preventive safeguards. The findings indicate that the respondents' perceptions of maturity in management practices related to IS planning, control, and organization are positively associated with their perceptions of IT security effectiveness.

The security of IT remains a complex matter, and the risk of breaches continues to be a problem (Richardson, 2003). However, this study's results would seem to indicate that current IT security safeguards are considered effective, at least by the sample of respondents who took part in this survey. Ongoing efforts are therefore required from both researchers and practitioners to determine an appropriate level of attention for this matter. In a time of heightened concern for security, management must assume accountability for the protection of vital IT assets, and ensure that protection for these assets is effective. To do so, it is important to strike a balance, avoiding overzealous protection of IS, while not succumbing to the "naïve belief that bad things only happen to other people" (Loch et al., 1992, p. 185). Moreover, given that mature IT infrastructure has become mission-critical to many modern organizations, Carr (2003) suggests that the next means of extracting strategic advantage from IS may be to focus attention on managing vulnerabilities rather than seeking new opportunities. Finally, the results

presented here imply that IT security practitioners should not underestimate the value of time spent in so-called soft-skill tasks, especially where they involve management control, organization, or planning activities.

References

Aladwani, A. M. (2002). Organizational actions, computer attitudes, and end-user satisfaction in public organizations: An empirical study. *Journal of End User Computing, 14*(1), 42-49.

Allen, B. (1968). Danger ahead! Safeguard your computer. *Harvard Business Review, 46*(6), 97-101.

Anthes, G. H. (1998, September 21). Lotsa talk, little walk. *Computerworld, 32*, 70-71.

Auer, T., & Ruohonen, M. (1997). Analysing the quality of IS use and management in the organizational context: Experience from two cases. *Information Resources Management Journal, 10*(3), 18-27.

Austin, R. D., & Darby, C. A. R. (2003). The myth of secure computing. *Harvard Business Review, 81*(6), 120-126.

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

Barclay, D., Higgins, C. A., & Thompson, R. (1995). The partial least squares (PLS) approach to causal modeling, personal computer adoption and use as an illustration. *Technology Studies, 2*(2), 285-309.

Benbasat, I., Dexter, A. S., Drury, D. H., & Goldstein, R. C. (1984). A critique of the stage hypothesis: Theory and empirical evidence. *Communications of the ACM, 27*, 476-485.

Benbasat, I., Dexter, A. S., & Mantha, R. W. (1980). Impact of organizational maturity on information system skill needs. *MIS Quarterly, 4*(1), 21-24.

Benbasat, I., & Zmud, R. W. (1999). Empirical research in information systems: The practice of relevance. *MIS Quarterly, 23*(1), 3-16.

Boynton, A. C., & Zmud, R. W. (1987). Information technology planning in the 1990's: Directions for practice and research. *MIS Quarterly, 11*(1), 59-71.

Brancheau, J. C., Janz, B. D., & Wetherbe, J. C. (1996). Key issues in information systems management: 1994-95 SIM delphi results. *MIS Quarterly, 20*(2), 225-242.

Briney, A., & Prince, F. (2002). Does size matter? 2002 ISM survey. *Information Security Magazine, 5*(9), 36-54.

Carr, N. G. (2003). IT doesn't matter. *Harvard Business Review, 81*(5).

Cheswick, W. R., & Bellovin, S. M. (1994). *Firewalls and internet security: Repelling the wily hacker*. Don Mills, Ontario, Canada: Addison-Wesley Publishing Company.

Chin, W. W. (1998). The partial least squares approach to structural equation modeling. In G. A. Marcoulides (Ed.), *Modern methods for business research* (pp. 295-336). Mahwah, NJ: Lawrence Erlbaum Associates.

Christie, V., & Goldman, J. (2003). *Measuring information security: Combining the SSE-CMM with the ISO 17799 standard* (No. ITP4667). Hershey, PA: Idea Group Publishing.

Churchill, N. C., Kempster, J. H., & Uretsky, M. (1969). *Computer-based information systems for management: A survey*. New York: National Association of Accountants.

COBIT: Control objectives. (3rd ed.)(2000). Rolling Meadows, IL: Information Systems Audit and Control Foundation.

Couper, M. P. (2000). Web surveys: A review of issues and approaches. *Public Opinion Quarterly, 64*(4), 464-494.

Courtney, R. H. J. (1977). Security risk assessment in electronic data processing systems. *Proceedings of the American Federation of Information Processing Societies National Computer Conference, Dallas TX, 46*, 97-104.

Daughtrey, T. (2001). Emerging issues in information security management. *Proceedings of the Quality Congress. ASQ's Annual Congress*, 406-412.

Dhillon, G. (2003). Data and information security. *Journal of Database Management, 14*(2), i - ii.

Dhillon, G. (Ed.). (2001). *Information security management: Global challenges in the new millennium*. Hershey, PA: Idea Group Publishing.

Dhillon, G., & Backhouse, J. (1996). Risks in the use of information technology within organizations. *Internation Journal of Information Management, 16*(1), 65-74.

Dillman, D. A. (2000). *Mail and internet surveys* (2nd ed.). Toronto, Ontario, Canada: John Wiley & Sons.

Drury, D. H. (1983). An empirical assessment of the stages of DP growth. *MIS Quarterly, 7*(2), 59-70.

Eloff, J. H. P. (1988). Computer security policy: Important issues. *Computers & Security, 7*(6), 559-562.

Farhoomand, F., & Gatehouse, M. (1988). Factors influencing the growth of the MIS department: A survey. *Journal of Information Systems Management, 5*, 56-60.

Ferneyhough, C. (2002, September 24). Canadian CEOs acknowledge own networks at risk but say preventing against threat not a priority. Retrieved January 5, 2004, from www.ipsos-reid.com

Fornell, C., & Larcker, D. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research, 18*, 39-50.

Galliers, R. D., & Sutherland, A. R. (1991). Information systems management and strategy formulation: The 'stages of growth' model revisited. *Journal of Information Systems, 1*(2), 89-114.

Gibson, C. F., & Nolan, R. L. (1974). Managing the four stages of EDP growth. *Harvard Business Review, 52*, 76-78.

Global information security survey 2002. (2002). Ernst & Young L.L.P.

Gollman, D., Meadows, C. A., & Okamoto, E. (2001). Editorial. *Internation Journal of Information Security, 1*, 1-2.

Goodhue, D. L., & Straub, D. W. (1991). Security concerns of system users: A study of perceptions of the adequacy of security. *Information & Management, 20*(1), 13-27.

Gopal, R. D., & Sanders, G. L. (1997). Preventive and deterrent controls for software piracy. *Journal of Management Information Systems, 13*(4), 29-47.

A guide to risk assessment and safeguard selection for information technology systems. (1996). Government of Canada, Communications Security Establishment.

A guide to security risk management for information technology systems. (1996). Government of Canada, Communications Security Establishment.

Gupta, Y. P., Karimi, J., & Somers, T. M. (1997). Alignment of a firm's competitive strategy and information technology management sophistication: The missing link. *IEEE Transactions on Engineering Management, 44*(4), 399-413.

Hair, J. F., Jr., Anderson, R. E., Tatham, R. L., & Black, W. C. (1998). *Multivariate data analysis* (5th ed.). Toronto, Ontario, Canada: Prentice-Hall.

Hoffer, J. A., & Straub, D. W. (1989). The 9 to 5 underground: Are you policing computer crimes? *Sloan Management Review, 30*(4), 35-44.

Igbaria, M., & Baroudi, J. J. (1995). The impact of job performance evaluations on career advancement prospects: An examination of gender differences in the IS workplace. *MIS Quarterly, 19*(1), 107-123.

Ilieva, J., Baron, S., & Healey, N. M. (2002). Online surveys in marketing research: Pros and cons. *International Journal of Marketing Research, 44*(3), 361-382.

ISO/IEC 17799:2000. Code of practice for information security management. (2000). Geneva: International Organization for Standardization.

Kankanhalli, A., Tan, B. C. Y., Teo, H. H., & Wei, K. K. (2003). An integrative study of information systems security effectiveness. *International Journal of Information Management, 23*(2), 139-154.

Kapica, J. (2003, June 10). Net security becoming corporate priority: Survey. *globeandmail.com*. Retrieved March 20, 2004, from http://www.globetechnology.com/servlet/story/RTGAM.20030610.gtsecurityjune10/BNStory/Technology

Karimi, J., Bhattacherjee, A., Gupta, Y. P., & Somers, T. M. (2000). The effects of MIS steering committees on information technology management sophistication. *Journal of Management Information Systems, 17*, 207-230.

Karimi, J., Gupta, Y. P., & Somers, T. M. (1996). Impact of competitive strategy and information technology maturity on firms' strategic response to globalization. *Journal of Management Information Systems, 12*, 55-88.

Karimi, J., Somers, T. M., & Gupta, Y. P. (2001). Impact of information technology management practices on customer service. *Journal of Management Information Systems, 17*(4), 125-158.

Keefe, P. (2003, February 10). Securing credibility. *Computerworld, 37*, 22.

King, J. L., & Kraemer, K. L. (1984). Evolution and organizational information systems: An assessment of Nolan's stage model. *Communications of the ACM, 27*, 466-259.

Landwehr, C. E. (2001). Computer security. *International Journal of Information Security, 1*, 3-13.

Loch, K. D., Carr, H. H., & Warkentin, M. E. (1992). Threats to information systems: Today's reality, yesterday's understanding. *MIS Quarterly, 17*(2), 173-186.

Lucas, H. C. J., & Sutton, J. A. (1977). The stage hypothesis and the s-curve: Some contradictory evidence. *Communications of the ACM, 20*, 254-259.

Machefsky, I. (1998). *A total economic impact analysis of two PKI vendors: Entrust and Verisign*. Norwell, MA: Giga Information Group.

McFarlan, E. W., McKenney, J. L., & Pyburn, P. (1983). The information archipelago - plotting a course. *Harvard Business Review, 61*(1), 145-156.

McQuillan, L. H. (2002). Security survey. *Executive Update, 3*(5).

Miles, R. E., & Snow, C. C. (1978). *Organizational strategy, structure and process*. New York: McGraw-Hill.

Morrel-Samuels, P. (2003). Web surveys' hidden hazards. *Harvard Business Review, 81*(7), 16-17.

Morton, C., & Froh, M. (1996, April). *Automating the assessment of risk in IT systems.* Paper presented at the Canadian Computer Security Symposium, Ottawa, Ontario, Canada.

Neumann, P. G. (1996). Risks in digital commerce. *Communications of the ACM, 39*(1), 154.

Nolan, R. L. (1973). Managing the computer resource: A stage hypothesis. *Communications of the ACM, 17*, 399-405.

Nolan, R. L. (1979). Managing the crises in data processing. *Harvard Business Review, 57*(2), 115-126.

Power, R. (2002). *2002 CSI/FBI computer crime and security survey*. Retrieved March 5, 2003, from http://www.gocsi.com/pdfs/fbi/FBI2002.pdf

Raho, L. E., Belohlav, J. A., & Fiedler, K. D. (1987). Assimilating new technology into the organization: An assessment of McFarlan and McKenney's model. *MIS Quarterly, 11*(1), 47-57.

Richardson, R. (2003). *2003 CSI/FBI computer crime and security survey*. Retrieved July 19, 2003, from http://www.gocsi.com/

Ross, J. W., & Weill, P. (2002). Six IT decisions your IT people shouldn't make. *Harvard Business Review, 80*(11), 85-91.

Sabherwal, R., & Kirs, P. (1994). The alignment between organizational critical success factors and information technology capability in academic institutions. *Decision Sciences, 25*(2), 301-330.

Siponen, M. (2002). Towards maturity of information security maturity criteria: Six lesson learned from software maturity criteria. *Information Management & Computer Security, 10*(5), 210-224.

Spafford, E. H. (1989). Crisis and aftermath. *Communications of the ACM, 32*, 678-687.

Stacey, T. R. (1996). The information security program maturity grid. *Information Systems Security, 5*(2), 22-33.

Straub, D. W. (1986a). Computer abuse and security: Update on an empirical pilot study. *Security Audit and Control Review, 4*(2), 21-31.

Straub, D. W. (1986b). *Deterring computer abuse: The effectiveness of deterrent countermeasures in the computer security environment.* Unpublished doctoral dissertation, Indiana University, Bloomington.

Straub, D. W. (1989). Validating instruments in MIS research. *MIS Quarterly, 13*(2), 147-169.

Straub, D. W. (1990a). Discovering and disciplining computer abuse in organizations: A field study. *MIS Quarterly, 14*(1), 45-60.

Straub, D. W. (1990b). Effective IS security: An empirical study. *Information Systems Research, 1*(3), 255-276.

Straub, D. W., & Welke, R. J. (1998). Coping with systems risk: Security planning models for management decision making. *MIS Quarterly, 22*(4), 441-469.

Sullivan, C. H., Jr. (1985). Systems planning in the information age. *Sloan Management Review, 26*, 3-11.

Systems security engineering capability maturity model (SSE-CMM). Model description document (version 3.0). (2003, June 15). Retrieved July 29, 2003, from http://www.sse-cmm.org/

Trcek, D. (2003). An integral framework for information systems security management. *Computers & Security, 22*(4), 337-360.

Troutt, M. D. (2002). IT security issues: The need for end user oriented research. *Journal of End User Computing, 14*(2), 48-49.

Vasishtha, P. (2002, September 9). VA's CIO takes over bureau's systems [Electronic version]. *Government Computer News, 21*(27). Retrieved March 20, 2003, from www.gcn.com

Verton, D. (2002, April 1). Disaster recovery planning still lags. *Computerworld, 36*, 10.

von Solms, B. (2001). Information security - A multidimensional discipline. *Computers & Security, 20*(6), 504-508.

Wood, C. C. (1987). Information systems security: Management success factors. *Computers & Security, 6*, 314-320.

Wylder, J. O. D. (1992). The life cycle of security managers: New responsibilities for a distributed environment. *Information Systems Management, 9*(1), 62-67.

Yoon, Y., Guimaraes, T., & O'Neal, Q. (1995). Exploring the factors associated with expert systems success. *MIS Quarterly, 19*(1), 83-106.

Appendix A

Survey Instrument

This appendix presents the research instrument used in this study. The following two tables (see Table 29 and Table 30) translate the construct items and the short item descriptions used throughout the text to the questions used in the questionnaire.

Table 29 Instrument questions for independent variable

Item	Item Description	Question Number
Maturity Integration 1	IT is strategic	23
Maturity Integration 2	Top down planning	24
Maturity Integration 3	IT in business units	25
Maturity Integration 4	New IT introduction	26
Maturity Organization 0	Ideas of IT personnel	28
Maturity Organization 1	Ideas of end users	29
Maturity Organization 2	IT knows business	30
Maturity Organization 3	IT group structure	31
Maturity Organization 4	End user relations	32
Maturity Control 1	IT direction authority	34
Maturity Control 2	IT operations authority	35
Maturity Control 3	IT proposals appraised	36
Maturity Control 4	IT performance	37
Maturity Control 5	Clear IT goals	38
Maturity Control 6	Clear IT performance	39
Maturity Planning 1	IT supports business	41
Maturity Planning 2	Examine IT innovation	42
Maturity Planning 3	Inform current IT	43
Maturity Planning 4	Inform potential IT	44
Maturity Planning 5	Org. informed about IT	45
Maturity Planning 6	IT project priorities	46

Table 30 Instrument questions for dependent variable

Item	Item Description	Question Number
Security 1	Security of hardware	10
Security 2	Security of software	11
Security 3	Security of data	12
Security 4	Security of services	13
Security 5	Deter insiders	14
Security 6	Deter outsiders	16
Security 7	Prevent insiders	15
Security 8	Prevent outsiders	17

The University of Lethbridge

You have 100% of the survey remaining

The University of Lethbridge
Faculty of Management

Survey of Canadian Information Systems Practitioner Views on Information Systems Management and Security

Dear IS Practitioner:

Thank you for contributing to this important all-Canadian research.

Rarely do practitioners have the opportunity to widely influence the important subject of Information Security. Even more rare is the chance to express a uniquely **Canadian** perspective. By participating in this study, you can directly affect how we understand the practice of IS management and security here in Canada.

This study is investigating how an organization's managerial practices affect the security of its Information Systems. The survey forms a key part of my Master's thesis at the University of Lethbridge in Alberta, and is purely a non-commercial, academic undertaking. **The survey should take approximately 20 minutes to complete**. **Please try to complete the entire survey in a single sitting**. If you log out, the survey will reset and you will have to start again from the beginning.

This website is only available until 18 July, so please ensure that you respond before then.

My contact information is below, should you wish to reach me for any reason. I have also included additional contacts, should you experience any difficulties with this survey.

Thank you for your participation,

Garry Spicer
M.Sc. (Management) Candidate
University of Lethbridge

UserID:

Password:

Start Survey

Contact Information		
Garry Spicer M.Sc. (Management) Candidate garry.spicer@uleth.ca (403) 381-7158	Linda Janz Faculty of Management Research Office janzli@uleth.ca (403) 329-2109	Jonathan Lane Technical Support lanej0@uleth.ca (403) 394-3924

The University of Lethbridge

You have 100% of the survey remaining

Context

There are no right or wrong answers in this survey. It is **your opinion** that matters. However, it is important that you have one organization in mind for the entire survey. The statements in this survey therefore refer to your perspectives and experiences at your **primary place of work**.

Your *primary place of work* depends on the type of IS practitioner you are:

- **If you are an employee of the organization for which you currently work:**
  - ***It is preferable* to use your current employer as your context for completing this questionnaire;**
  - ***Alternatively*, you may use a previous employer as your context for completing this questionnaire, if you have recently started work with a new organization and are not yet familiar with this new organization.**
- **If you are a consultant or contractor:**
  - ***It is preferable* to use a client organization with which you have become familiar as your context for completing this questionnaire;**
  - ***Alternatively*, you may use the consulting or contracting firm for which you work as your context for completing this questionnaire.**

It is very important that you use a single organization as your primary place of work for the entire survey. Additionally, if there are multiple IS teams at your primary place of work, then please consider the questions in this survey from the perspective of the IS team with which you are the most familiar.

Definitions

This survey uses the following definitions:

- *IS* is a short form for Information System or Information Systems;
- *IT* is a short form for Information Technology;
- *IS* and *IT* are used interchangeably for the purposes of this survey;
- *Information Security*, *IT Security*, and *IS Security* have the same meaning: protecting IS-related hardware, software, data, and services from deliberate, accidental, or random threats to confidentiality, integrity, or availability. This includes physical, electronic, personnel, and policy measures.

Confidentiality and Ethics

All information you provide in this survey will be held in strict confidence. It will be used only for the purpose of studying IS management and security. My research team and I will be the only ones with access to the raw data, and only aggregate information will be reported. The raw data will not be given, sold, or made accessible to any third parties.

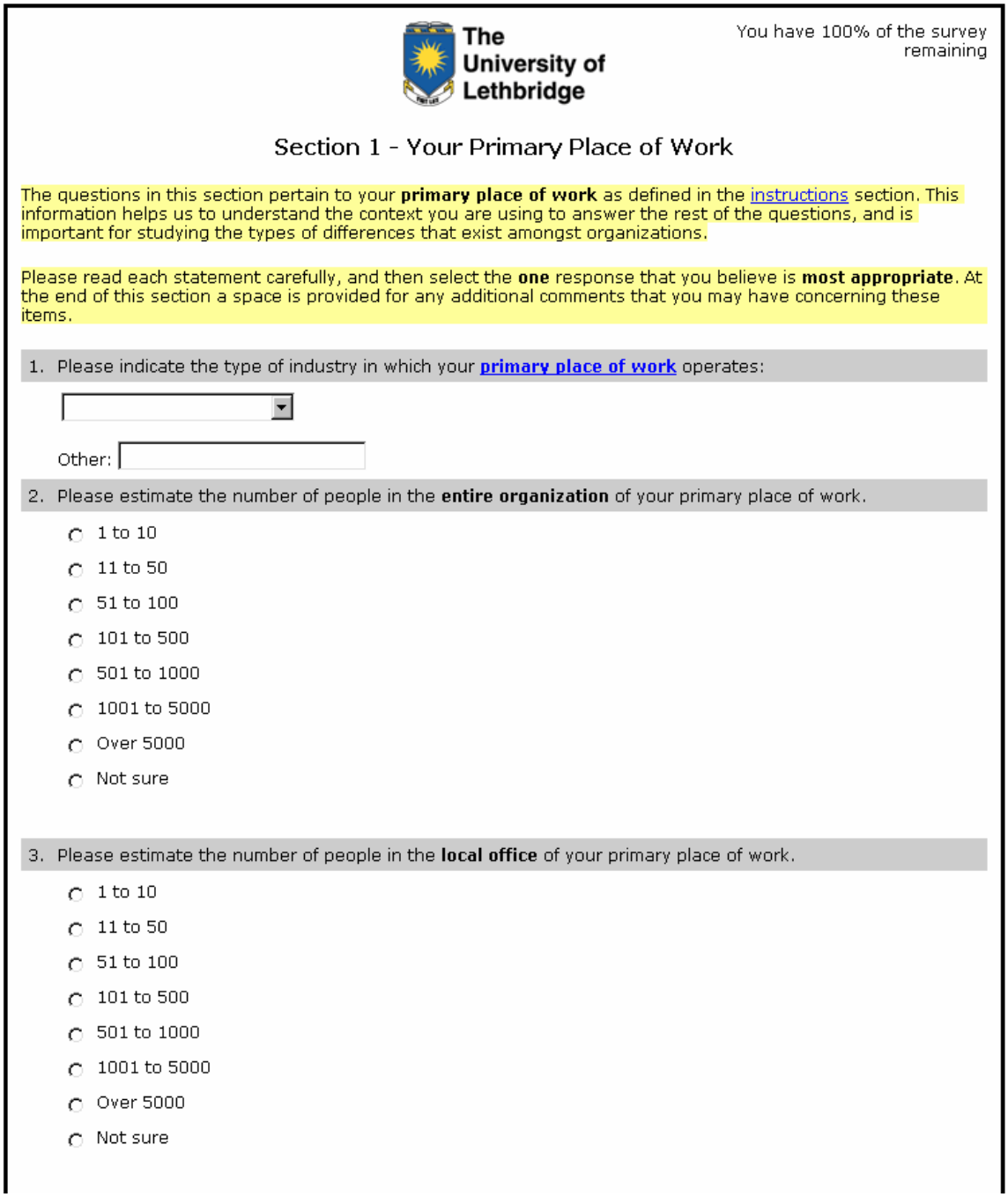
This survey does *not* request any sensitive technical information (e.g. your firewall configuration). Neither are there any questions that concern confidential details about security incidents in your organization. Rather, I am asking you to provide your beliefs about organizational IS management and overall security effectiveness.

Your participation in this survey is completely voluntary, and you may withdraw if you choose to do so. You may elect to not answer a question, and you may opt to remain anonymous if you so choose. The Faculty of Management Research and Ethics Committee at The University of Lethbridge has reviewed this project to ensure its compliance with acceptable research practices, including confidentiality of data.

Completion

The survey should take approximately 20 minutes to complete. **Please try to complete the entire survey in a single sitting**. If you log out, the survey will reset and you will have to start again from the beginning.

Next Page



The University of Lethbridge

You have 100% of the survey remaining

Section 1 - Your Primary Place of Work

The questions in this section pertain to your **primary place of work** as defined in the instructions section. This information helps us to understand the context you are using to answer the rest of the questions, and is important for studying the types of differences that exist amongst organizations.

Please read each statement carefully, and then select the **one** response that you believe is **most appropriate**. At the end of this section a space is provided for any additional comments that you may have concerning these items.

1. Please indicate the type of industry in which your **primary place of work** operates:

Other:

2. Please estimate the number of people in the **entire organization** of your primary place of work.

- 1 to 10
- 11 to 50
- 51 to 100
- 101 to 500
- 501 to 1000
- 1001 to 5000
- Over 5000
- Not sure

3. Please estimate the number of people in the **local office** of your primary place of work.

- 1 to 10
- 11 to 50
- 51 to 100
- 101 to 500
- 501 to 1000
- 1001 to 5000
- Over 5000
- Not sure

4. Please estimate the number of people who are part of the **organization-wide IS group** of your primary place of work.

- ○ 1 to 10
- ○ 11 to 50
- ○ 51 to 100
- ○ 101 to 500
- ○ Over 500
- ○ Not sure

5. Which of the following best describes how **responsibility for overall IS management** is assigned at your primary place of work?

   The **most senior** person **within the IS group** reports to:

- ○ The organization's top officer (e.g. President or Deputy Minister).
- ○ An **executive manager** (e.g. a Vice President) who is responsible for more than just IS.
- ○ A manager who is responsible for more than just IS.
- ○ Not sure

6. Within your primary place of work, how influential within the organization is the **most senior** person **within the IS group**?

- ○ Not at all influential
- ○ Only slightly influential
- ○ Moderately influential
- ○ Substantially influential
- ○ Extremely Influential
- ○ Not sure

7. Which of the following best describes how **responsibility for IS security** is assigned at your primary place of work:

   The **most senior** person responsible for **IS security** reports to:

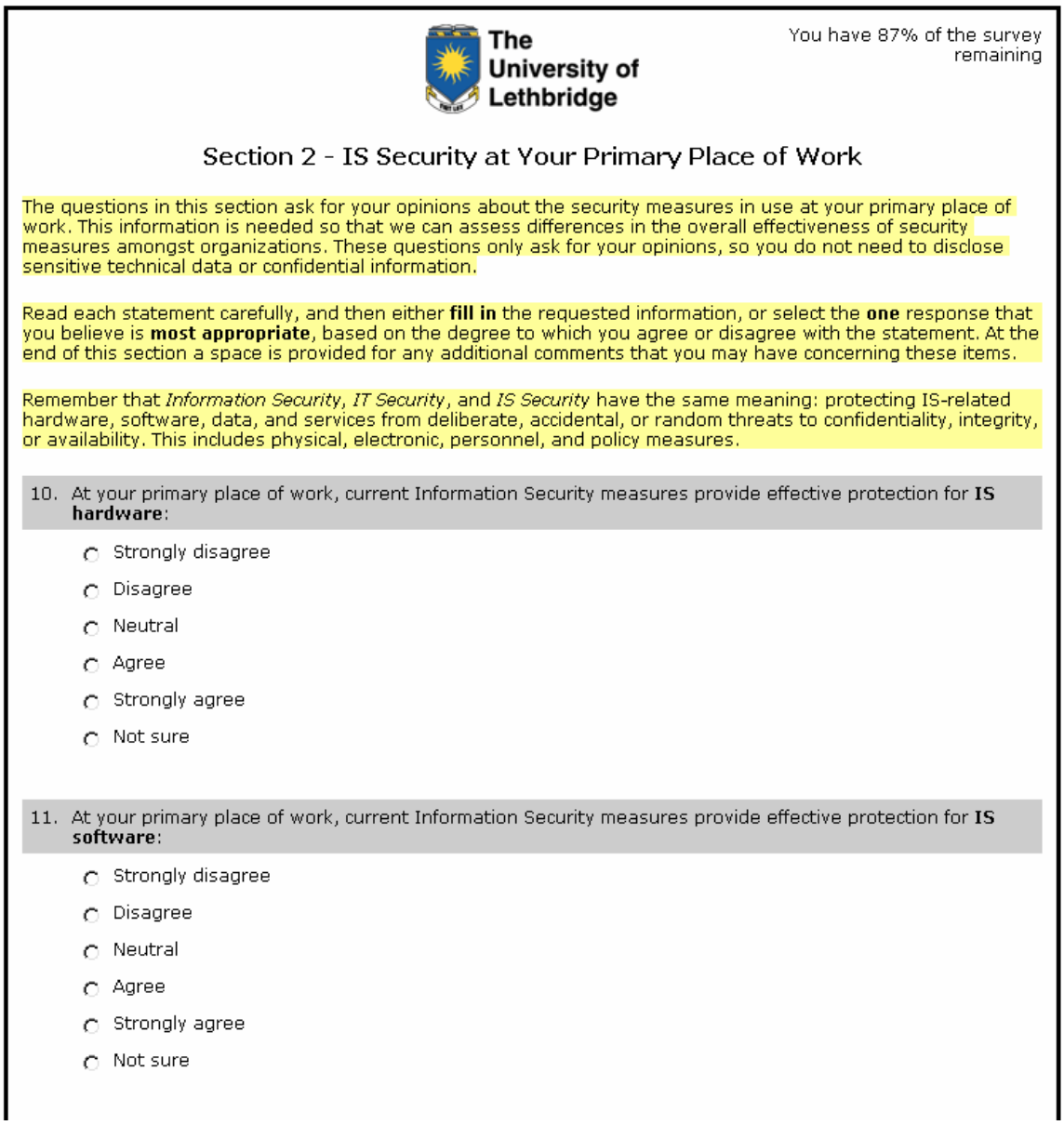
- ○ The organization's top officer. (e.g. President or Deputy Minister)
- ○ An **executive manager** within the IS group. (e.g. a Vice President IS or CIO)
- ○ An **executive manager** outside the IS group. (e.g. a Vice President Finance or Operations)
- ○ A manager within the IS group.
- ○ A manager outside of the IS group.
- ○ Responsibility for IS security is distributed amongst several people or is determined on a per-project basis.
- ○ Responsibility for IS security is not assigned to anyone.
- ○ Not sure

8. Within your primary place of work, how influential within the organization is the **most senior** person responsible for **IS security**?

- ○ Not at all influential
- ○ Only slightly influential
- ○ Moderately influential
- ○ Substantially influential
- ○ Extremely influential
- ○ Responsibility for IS security is distributed amongst several people or is determined on a per-project basis.
- ○ Responsibility for IS security is not assigned to anyone.
- ○ Not sure

9. (Optional) Do you have any additional comments on the items in this section?

Next Page


The University of Lethbridge

You have 87% of the survey remaining

Section 2 - IS Security at Your Primary Place of Work

The questions in this section ask for your opinions about the security measures in use at your primary place of work. This information is needed so that we can assess differences in the overall effectiveness of security measures amongst organizations. These questions only ask for your opinions, so you do not need to disclose sensitive technical data or confidential information.

Read each statement carefully, and then either **fill in** the requested information, or select the **one** response that you believe is **most appropriate**, based on the degree to which you agree or disagree with the statement. At the end of this section a space is provided for any additional comments that you may have concerning these items.

Remember that *Information Security*, *IT Security*, and *IS Security* have the same meaning: protecting IS-related hardware, software, data, and services from deliberate, accidental, or random threats to confidentiality, integrity, or availability. This includes physical, electronic, personnel, and policy measures.

10. At your primary place of work, current Information Security measures provide effective protection for **IS hardware**:

- ○ Strongly disagree
- ○ Disagree
- ○ Neutral
- ○ Agree
- ○ Strongly agree
- ○ Not sure

11. At your primary place of work, current Information Security measures provide effective protection for **IS software**:

- ○ Strongly disagree
- ○ Disagree
- ○ Neutral
- ○ Agree
- ○ Strongly agree
- ○ Not sure

12. At your primary place of work, current Information Security measures provide effective protection for **electronic data**:

- Strongly disagree
- Disagree
- Neutral
- Agree
- Strongly Agree
- Not sure

13. At your primary place of work, current Information Security measures provide effective protection for **the services provided by Information Systems** (e.g. file, print, e-mail services):

- Strongly disagree
- Disagree
- Neutral
- Agree
- Strongly agree
- Not sure

14. At your primary place of work, current Information Security measures are effective in **deterring** security violations by **insiders** (i.e. discouraging **known/internal people** from attempting to breach the organization's security measures):

- Strongly disagree
- Disagree
- Neutral
- Agree
- Strongly agree
- Not sure

15. At your primary place of work, current Information Security measures are effective in **preventing** security violations by **insiders** (i.e. stopping attempts by **known/internal people** from actually breaching the organization's security measures):

- Strongly disagree
- Disagree
- Neutral
- Agree
- Strongly agree
- Not sure

16. At your primary place of work, current Information Security measures are effective in **deterring** security violations by **outsiders** (i.e. discouraging **unknown/external people** from attempting to breach the organization's security measures):

- Strongly disagree
- Disagree
- Neutral
- Agree
- Strongly agree
- Not sure

17. At your primary place of work, current Information Security measures are effective in **preventing** security violations by **outsiders** (i.e. stopping attempts by **unknown/external people** from actually breaching the organization's security measures):

- Strongly disagree
- Disagree
- Neutral
- Agree
- Strongly agree
- Not sure

18. Overall, current Information Security measures at your primary place of work are effective.

- Strongly disagree
- Disagree
- Neutral
- Agree
- Strongly agree
- Not sure

19. The **IS security policy** at your primary place of work is **comprehensive**.

- Strongly disagree
- Disagree
- Neutral
- Agree
- Strongly agree
- There is no security policy
- Not sure

20. The **IS security policy** at your primary place of work is **thoroughly implemented**.

- Strongly disagree
- Disagree
- Neutral
- Agree
- Strongly agree
- There is no security policy
- Not sure

21. What do you believe most directly influences the effectiveness of Information Security measures in your organization?

22. (Optional) Do you have any additional comments on the items in this section?

Next Page

The University of Lethbridge

You have 67% of the survey remaining

Section 3 - IS Management at Your Primary Place of Work

The questions in this section ask you to describe your opinions about the management practices in use at your primary place of work. This information is used to understand and assess differences in the way organizations manage Information Systems.

Please read each statement carefully, then select the **one** response that you believe is **most appropriate**, based on the degree to which you agree or disagree with the statement. There are four parts to this section. At the end of each part a space is provided for any additional comments that you may have concerning the items there.

Section 3 - Part A

23. At your primary place of work, top management perceives that future use of IT is of strategic importance.

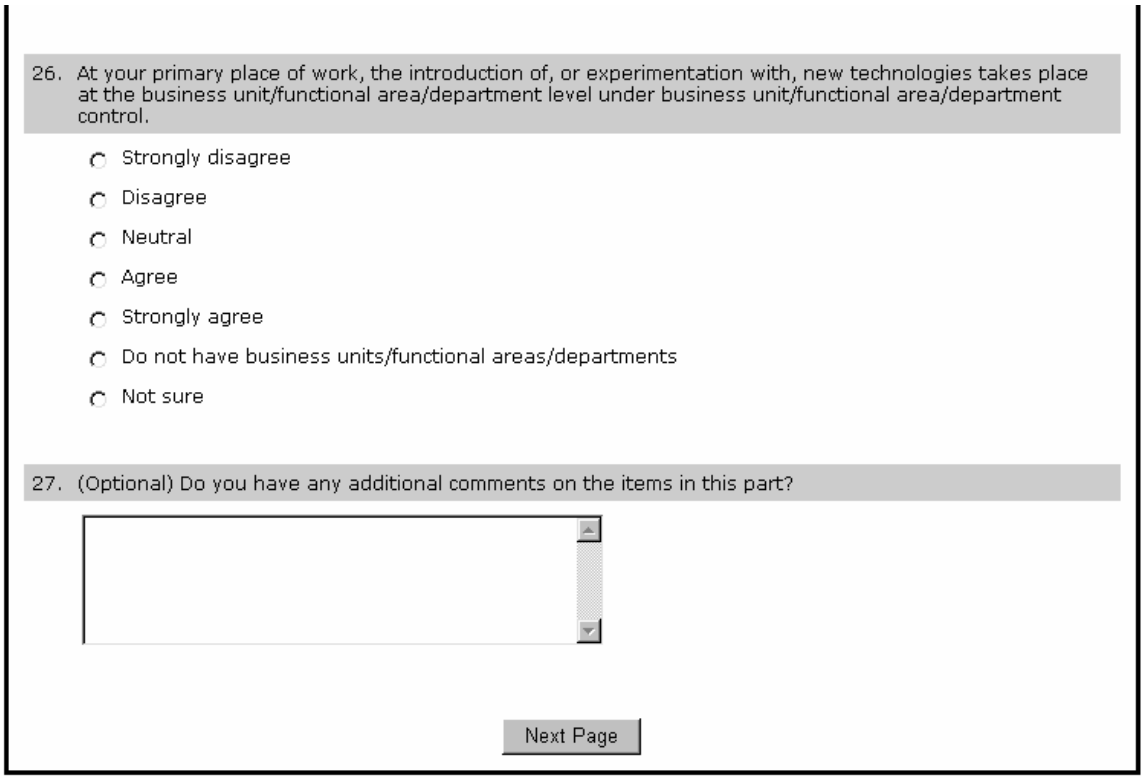
- ○ Strongly disagree
- ○ Disagree
- ○ Neutral
- ○ Agree
- ○ Strongly agree
- ○ Not sure

24. At your primary place of work, there is a top-down planning process for linking IT strategy to business needs.

- ○ Strongly disagree
- ○ Disagree
- ○ Neutral
- ○ Agree
- ○ Strongly agree
- ○ Not sure

25. At your primary place of work, some IT development resources are positioned within individual business units/functional areas/departments.

- ○ Strongly disagree
- ○ Disagree
- ○ Neutral
- ○ Agree
- ○ Strongly agree
- ○ Do not have business units/functional areas/departments
- ○ Not sure



The University of Lethbridge

You have 60% of the survey remaining

Section 3 - Part B

28. At your primary place of work, the ideas of IT personnel are given due attention in IT planning and implementation.

- Strongly disagree
- Disagree
- Neutral
- Agree
- Strongly agree
- Not sure

29. At your primary place of work, end user ideas are given due attention in IT planning and implementation.

- Strongly disagree
- Disagree
- Neutral
- Agree
- Strongly agree
- Not sure

30. At your primary place of work, the IT personnel understand the business and the organization.

- Strongly disagree
- Disagree
- Neutral
- Agree
- Strongly agree
- Not sure

31. At your primary place of work, the structure of the IT group fits the organization.

- Strongly disagree
- Disagree
- Neutral
- Agree
- Strongly agree
- Not sure

32. At your primary place of work, relations between IT personnel and end users are constructive.

- Strongly disagree
- Disagree
- Neutral
- Agree
- Strongly agree
- Not sure

33. (Optional) Do you have any additional comments on the items in this part?

Next Page

The University of Lethbridge

You have 52% of the survey remaining

Section 3 - Part C

34. At your primary place of work, the overall responsibility and authority for IT direction and development are clear.

- Strongly disagree
- Disagree
- Neutral
- Agree
- Strongly agree
- Not sure

35. At your primary place of work, the overall responsibility and authority for IT operations are clear.

- Strongly disagree
- Disagree
- Neutral
- Agree
- Strongly agree
- Not sure

36. At your primary place of work, IT project proposals are properly appraised.

- Strongly disagree
- Disagree
- Neutral
- Agree
- Strongly agree
- Not sure

37. At your primary place of work, the organization regularly monitors the performance of its IT functions.

- Strongly disagree
- Disagree
- Neutral
- Agree
- Strongly agree
- Not sure

38. At your primary place of work, the IT group is clear about its goals and responsibilities.

- Strongly disagree
- Disagree
- Neutral
- Agree
- Strongly agree
- Not sure

39. At your primary place of work, the IT group is clear about its performance criteria.

- Strongly disagree
- Disagree
- Neutral
- Agree
- Strongly agree
- Not sure

40. (Optional) Do you have any additional comments on the items in this part?

Next Page

The University of Lethbridge

You have 42% of the survey remaining

Section 3 - Part D

41. At your primary place of work, the IT projects support the organization's business objectives and strategies.

- Strongly disagree
- Disagree
- Neutral
- Agree
- Strongly agree
- Not sure

42. At your primary place of work, the organization regularly examines the innovative opportunities that IT can provide for competitive advantage.

- Strongly disagree
- Disagree
- Neutral
- Agree
- Strongly agree
- Not sure

43. At your primary place of work, the organization is adequately informed about the **current** use of IT by competitive forces (e.g. buyers, suppliers, and competitors) in its industry.

- Strongly disagree
- Disagree
- Neutral
- Agree
- Strongly agree
- Not sure

44. At your primary place of work, the organization is adequately informed about the **potential** use of IT by competitive forces (e.g. buyers, suppliers, and competitors) in its industry.

- Strongly disagree
- Disagree
- Neutral
- Agree
- Strongly agree
- Not sure

45. At your primary place of work, the organization has adequate information about the capabilities and quality of its IT systems.

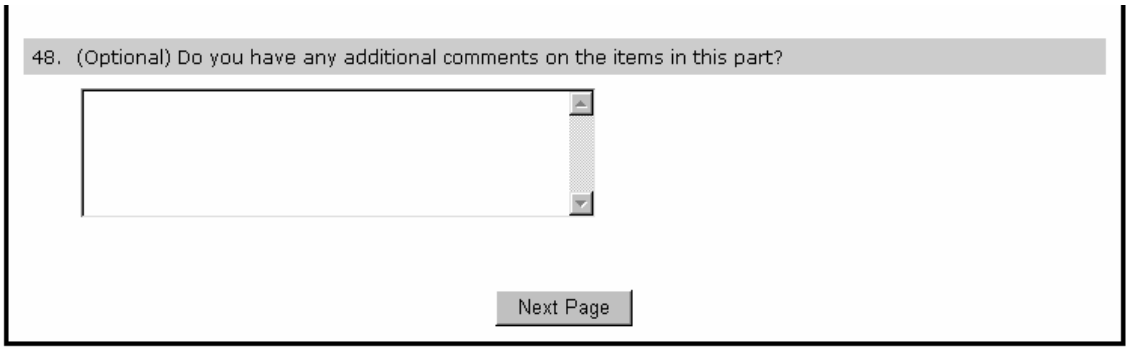
- Strongly disagree
- Disagree
- Neutral
- Agree
- Strongly agree
- Not sure

46. At your primary place of work, the organization is satisfied with how its IT project priorities are set.

- Strongly disagree
- Disagree
- Neutral
- Agree
- Strongly agree
- Not sure

47. At your primary place of work, IS is managed effectively.

- Strongly disagree
- Disagree
- Neutral
- Agree
- Strongly agree
- Not sure



The University of Lethbridge

You have 30% of the survey remaining

Section 4 - General Questions

The items in this section ask specific questions about you and your **primary place of work**. This information is important for studying the ways in which different people understand IS management and security.

Please read each statement carefully, and then either **fill in** the requested information, or select the response or responses that you believe to be **most appropriate** for that statement. At the end of this section a space is provided for any additional comments that you may have concerning these items.

49. Which of the following best describes you?

- ○ I am self-employed.
- ○ I work for a consulting/contracting firm.
- ○ I am a full or part time employee at my primary place of work.
- ○ Other (Please specify)

50. Which of the following best describes your primary place of work, as your context for this survey?

- ○ My primary place of work is my employer.
- ○ My primary place of work is a former employer.
- ○ My primary place of work is a client organization.
- ○ Other (Please specify)

51. Considering your primary place of work, which of the following best describes the office in which you were/are based?

- ○ Main Location or Head Office (National or International)
- ○ Divisional Head Office
- ○ Regional Head Office
- ○ Local Office
- ○ Remote Office or Field Location
- ○ Home (Residential) Office
- ○ Other (Please specify)

52. What is your **current, or most recent**, position at your primary place of work?

- ○ Executive or senior management (e.g. director, senior manager, CIO, or VP)
- ○ Management (with control over a capital or operational budget)
- ○ Supervisor (e.g. project manager or team leader)
- ○ Technical (e.g. programmer, analyst, technician/technologist)
- ○ Student (including co-op education and practicum students)
- ○ Other (Please specify)

53. How long have/had you worked for this organization?

Years:
Months:

54. How long have/had you been in your **most recent position** with this organization?

Years:
Months:

55. Please indicate your **primary** area of IS related expertise:

- ○ Technology (e.g. networks, operating systems, hardware)
- ○ Applications (e.g. software design/development/maintenance/deployment)
- ○ Database (e.g. database design, implementation, maintenance, support)
- ○ Security/Privacy (e.g. computer/network security, Information security/privacy)
- ○ Management (e.g. line management, project management, business process design)
- ○ Other (Please specify)

56. What percentage of your time is spent on security issues? (0 to 100)

57. To which of the following professional organizations do you **currently** belong? (**Check all that apply**.)

- ☐ CIPS
- ☐ SPIE
- ☐ ISSA
- ☐ ISACA
- ☐ None of the above

58. Which of the following security practitioner credentials do you **currently** hold? (**Check all that apply**.)

- ☐ CISSP
- ☐ SSCP
- ☐ CISA
- ☐ GSE
- ☐ None of the above
- ☐ Other (Please specify)

59. Please indicate your gender.

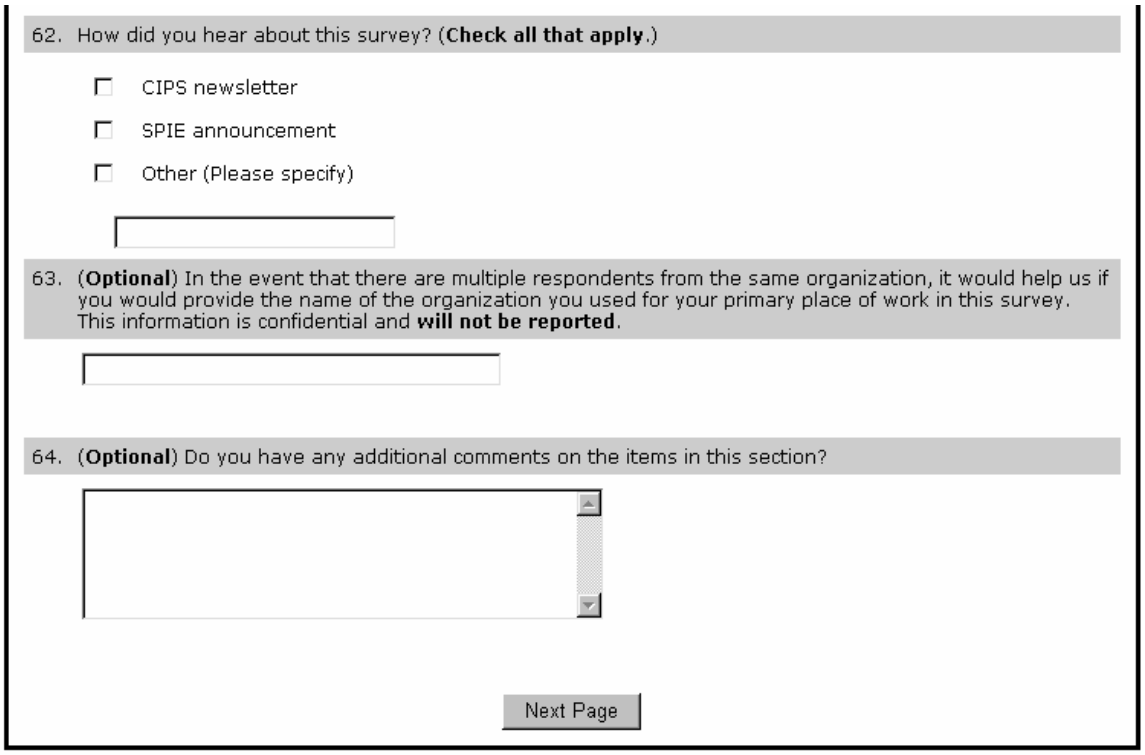
- ○ Male
- ○ Female

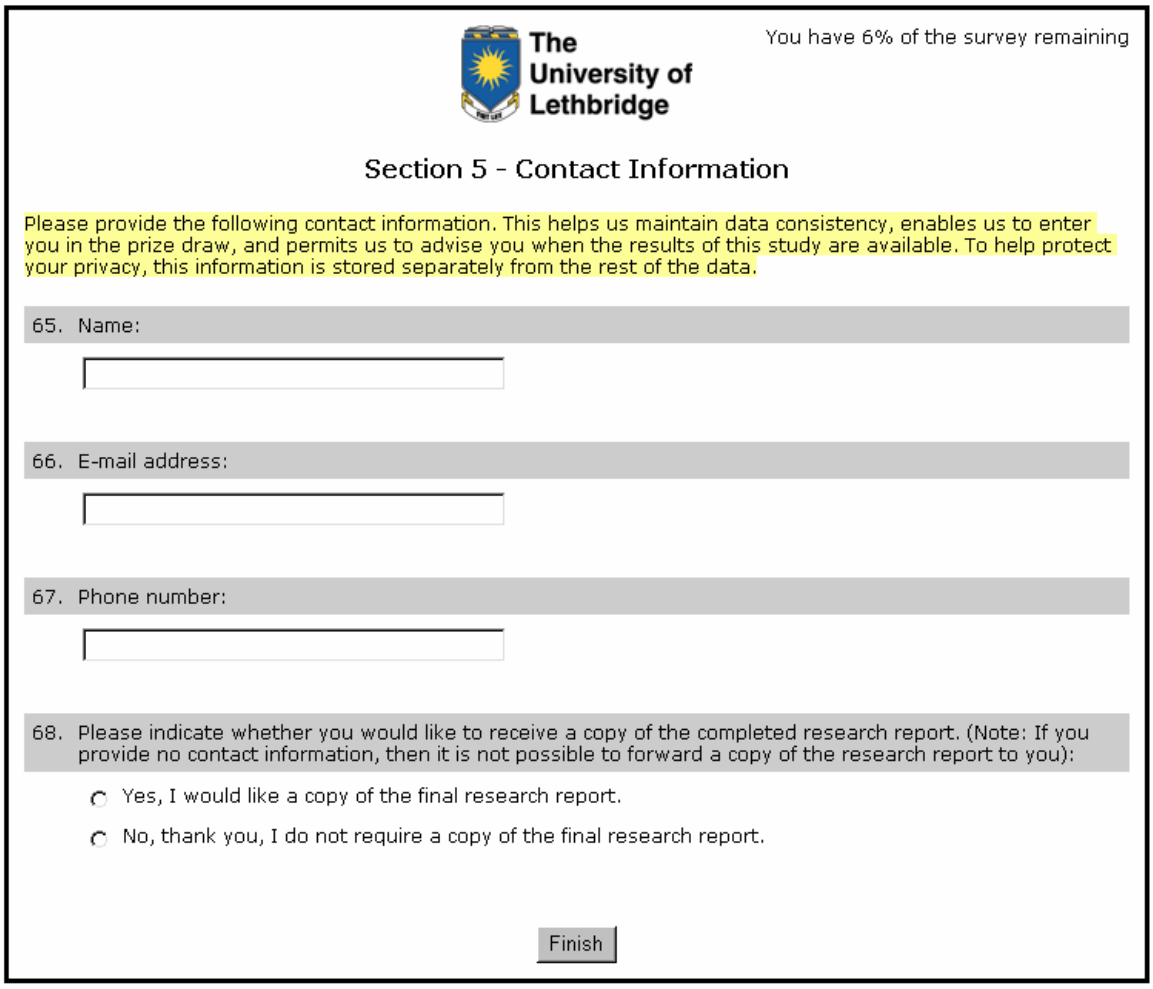
60. Please indicate your age.

- ○ Under 20
- ○ 20 to 24
- ○ 25 to 29
- ○ 30 to 34
- ○ 35 to 39
- ○ 40 to 44
- ○ 45 to 49
- ○ 50 to 54
- ○ 55 to 59
- ○ 60 or over

61. Please indicate the highest level of education that you have **completed**.

- ○ Some High School
- ○ Completed High School
- ○ Completed Post Secondary Certificate
- ○ Some College
- ○ Completed College
- ○ Some University
- ○ Completed University
- ○ Some Graduate Work
- ○ Completed Graduate Work
- ○ Other (Please specify)





Section 6 - Thank You

Thank you for your time and your careful consideration of the questions in this survey. The information you provided is vital to improving our understanding of IS management and security. Please be assured that all individual responses will remain confidential, and will not be made available to anyone but my research committee and me. The analysis should be complete in a few months, and if you requested a copy of the study it will be made available to you at that time. If you have any questions in the mean time, please feel free to contact me: garry.spicer@uleth.ca.

Best Regards,

Garry Spicer
M.Sc. in Management Candidate (2003)
University of Lethbridge,
Lethbridge Alberta

To end your session and ensure that your entries are properly recorded, please close your browser now.

Appendix B

Survey Notices and Reminders

An Opportunity to Influence IS Security Practices in Canada

Despite all the attention paid to IS security in recent years, little consideration has been given to what **you**, the Canadian IS practitioner, have to say about this important issue. Here is a unique opportunity to express your opinions about the ways in which IS management practices affect IS security, and to see how your views compare with those of other *Canadian* IS practitioners.

I invite you to participate in an upcoming study on how IS management practices affect IS security. It will only take about 20 minutes of your time, and **you will not be asked to provide any sensitive technical information or confidential details about your organization's security practices**. The survey forms a key part of my Master's thesis at The University of Lethbridge in Alberta, and is purely a non-commercial, academic undertaking. As a participant, you are entitled to a free copy of the final report that can be shared openly and used to compare your ideas with those of other Canadian IS practitioners. I will respond to any specific queries that you may have about the study or its findings, and every participant is eligible to participate in a draw for a valuable gift certificate.

I am currently preparing an online questionnaire that will be straightforward and easy to use. There will be measures in place to properly protect the information you provide, and it will be used only for the purpose of academic research into IS management and security. Additionally, The Faculty of Management Research and Ethics Committee at The University of Lethbridge has reviewed this study for conformance to acceptable ethical guidelines and standards.

I will be announcing the survey in approximately two weeks (on or about 20 June), at which time the link to the questionnaire site will be made available to you. I hope that you will be part of this important study. If you have any questions, please contact me at the email address provided below.

Thank you,
Garry Spicer
M.Sc. (Mgt) Candidate
The University of Lethbridge
Garry.Spicer@Uleth.ca

Study on IS Management and IS Security Effectiveness in Canada

Despite all the attention paid to IS security in recent years, little consideration has been given to what **you**, the Canadian IS practitioner, have to say about this important issue. Here is a unique opportunity to express your opinions about the ways in which IS management practices affect IS security, and to see how your views compare with the aggregated perspectives of other *Canadian* IS practitioners.

The web survey is straightforward and easy to use, so I invite you to participate by following the link provided below. It will only take about 20 minutes of your time, and **you will not be asked to provide any sensitive technical information**. There are measures in place to make certain that the information you provide is properly protected, and it will be used strictly for the purposes of academic research into IS management and IS security. This study has been considered and approved by The Faculty of Management Research and Ethics Committee at The University of Lethbridge, and conforms to acceptable ethical guidelines and standards as described in the Tri-Council Policy Statement for the ethical conduct of research involving humans.

This important research will help us to better understand how to improve Information Systems management and security here in Canada. As a participant, you are entitled to a **free** copy of the study results, which you may find useful for comparing your views to averages from across the country. Additionally, I will respond to any specific queries that you may have about the report's contents. Finally, every one who completes a survey is eligible to participate in a draw for one of four $50 gift certificates from <deleted>.

To complete the survey, please follow this link (you will need the ID and Password, below):

http://fusion.uleth.ca/crdc/spicer_survey/

Userid: <deleted>
Password: <deleted>

If you have any questions or concerns, please contact me at the email address provided below.

Thank you,
Garry Spicer
M.Sc. (Mgt) Candidate
The University of Lethbridge
Garry.Spicer@Uleth.ca

Reminder: Study on IS Management and IS Security Effectiveness in Canada

In a previous message, I invited you to provide your input to this important study on how IS management practices influence IS security effectiveness. If you have already completed the online questionnaire, then I thank you for your time and wish you the best of luck in the prize draw that will take place soon after the survey web site is closed. However, if you have not yet completed the survey, then I hope you will consider doing so. It will only take about 20 minutes of your time, and **you will not be asked to provide any sensitive technical information**.

This valuable research will help us to better understand how to improve Information Systems management and security here in Canada. As a participant, you are entitled to a **free** copy of the study results, which you may find useful for comparing your views to averages from across the country. Additionally, I will respond to any specific queries that you may have about the report's contents.

The web survey is straightforward and easy to use, so I invite you to participate by following the link below. There are measures in place to protect the information you provide, and it will be used strictly for the purposes of academic research into IS management and security. This study has been considered and approved by The Faculty of Management Research and Ethics Committee at The University of Lethbridge.

The survey web site closes on 18 July, so be sure to take advantage of this opportunity before then. Finally, do not forget that every one who completes a survey is eligible to participate in a draw for one of four $50 gift certificates from <deleted>.

To complete the survey, please follow this link (you will need the ID and Password, below):

http://fusion.uleth.ca/crdc/spicer_survey/

Userid: <deleted>
Password: <deleted>

If you have any questions or concerns, please contact me at the email address provided below.

Thank you,
Garry Spicer
M.Sc. (Mgt) Candidate
The University of Lethbridge
Garry.Spicer@Uleth.ca