A COMPARISON OF INFORMATION SECURITY TRENDS BETWEEN FORMAL AND INFORMAL ENVIRONMENTS

Except where reference is made to the work of others, the work described in this dissertation is my own or was done in collaboration with my advisory committee. This dissertation does not include proprietary or classified information.

James Emory Ryan

Certificate of Approval:

Nelson Ford
Associate Professor
Management

Kelly Rainer, Chair
Professor
Management

Tom Marshall
Associate Professor
Management

Stephen L. McFarland
Dean
Graduate School

A COMPARISON OF INFORMATION SECURITY TRENDS BETWEEN FORMAL AND INFORMAL ENVIRONMENTS

James Emory Ryan

A Dissertation

Submitted to

the Graduate Faculty of

Auburn University

in Partial Fulfillment of the

Requirements for the

Degree of

Doctor of Philosophy

Auburn, Alabama
August 7, 2006

A COMPARISON OF INFORMATION SECURITY TRENDS BETWEEN FORMAL AND INFORMAL ENVIRONMENTS

James Emory Ryan

____
Signature of Author

August 7, 2006
Date of Graduation

DISSERTATION ABSTRACT

A COMPARISON OF INFORMATION SECURITY TRENDS BETWEEN FORMAL AND INFORMAL ENVIRONMENTS

James Emory Ryan

Doctor of Philosophy, August 7, 2006
(M.M.I.S Auburn University, 2001)
(B.S. Auburn University, 1981)

317 Typed Pages

Directed by Kelly Rainer

The study compared the awareness and practice of information security between formal and informal computing-environments. This study was conducted to develop a measurement instrument for user-level awareness and practice of information security and establish a foundation upon which further research could be based. The study results included a delineation of the information security awareness domain, a tested measurement instrument, a tested model for user-level information security awareness, and a statistical profile of user-level information security awareness and practice among employees of a public research university.

Characteristics which represent the operational definition of information security awareness and practice were found to be: personal innovativeness, computer self-efficacy, individual awareness, formal practice, and informal practice. Individual awareness was measured over perspectives of technology, policy, and threat-context. Formal practice was measured over perspectives of deterrent, preventive, and combined deterrent-preventive efforts. Informal practice was measured over perspectives of access control, physical protection, user authentication, security management, and encryption. Established scales were used to measure personal innovativeness and computer self-efficacy. The measurement instrument also included demographic variables and technology variables between computing-environments. All of these characteristics were considered ISA domain measures and were included in the developed measurement instrument.

The extent of user-level information security awareness was supported by the measure to which these characteristics were acknowledged by individual computer users. A sample of 531 university employees indicated that the measurement instrument exhibited acceptable properties of reliability and validity. The survey data showed that the university employees had information security awareness to some extent. Also, the sample data had satisfactory fit within the research model.

The study's results supported the research model hypotheses. Personal innovativeness and computer self-efficacy had direct, positive relationships with individual awareness. Individual awareness mediated personal innovativeness and computer self-efficacy over direct, positive relationships with formal and informal practice. Formal practice mediated individual awareness over a direct, positive relationship with informal practice. The study's results also indicated demographic and technology known-groups had effects over the ISA domain measures.

ACKNOWLEDGEMENTS

With all my respect, admiration, and appreciation I would like to acknowledge the members of my doctoral committee, for their vast knowledge, time, and patience. I would especially like to thank Dr. Kelly Rainer who read my draft copies, originally encouraged my pursuit of a Ph.D., and was an invaluable mentor. I would like to thank Dr. Tom Marshall for his unwavering support and expertise throughout my graduate studies. Also, I would like to thank Dr. Nelson Ford for all his faith, support, and advice.

I wish to acknowledge my wife, Janice Dobbs Ryan, for her loving encouragement, counsel, and steadfast support (Philippians 1:3). To my children, Chase and Mary Elizabeth, thank you for the pleasure you always give me, especially throughout this journey. I hope my example will assist each of you in obtaining your educational goals. I also acknowledge my mother and late father, Frances Elizabeth and C. P. Ryan, for their encouragement, support, and appreciation of all my educational aspirations through the years.

Style manual or journal used Publication Manual of the American Psychological Association, 5th Edn.

Computer software used Microsoft Word XP; SPSS v.11; GPOWER v. 2; Microsoft Excel XP; Microsoft PowerPoint XP; AMOS v. 5; GroupWise v. 6.5

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER I. INTRODUCTION

Authors have postulated that information security is a learned behavior (Thomson and von Solms, 1998, 2005; Leach, 2003; Schou and Trimmer, 2004), which increases the merit in optimizing the learned behavior required for sufficiency (Straub, 1990; Straub and Nance, 1990; Straub and Welke, 1998; Menascé, 2003; Sandhu, 2003; Aytes and Connolly, 2004; Stahl, 2004; Ma and Pearson, 2005; Stanton, Stam, Mastrangelo, and Jolton, 2005). However, learning requires knowledge transfer from formal and/or informal training channels to complete the knowledge transfer tasks (Kanter, 2003; Wu and Rocheleau, 2001). These views are highly relevant to information security where the absence of appropriate formal and/or informal training channels yields insufficient outcomes (Leach, 2003; Stanton, Stam, Mastrangelo, and Jolton, 2005).

Information security also presents a perception challenge because threats to information security are dynamic (Kruger and Kearney, 2006). Furthermore, individual perceptions influence individual beliefs about the value of a technology (Lewis, Agarwal, and Sambamurthy, 2003). Thus, these relevant views provide a foundation for investigating the operationalization of information security into awareness and practice.

Information security awareness results in security practice, which protects information and information systems. However, information security awareness has differing developmental origins (Straub, 1990). Also, differing information security awareness yields information security with differing security practice (Kankanhalli, Teo, Tan, and Wei, 2003). Hence, further development of salient information security issues between awareness and practice is justified (Aytes and Connolly, 2004).

The following example offers support to the current industry trends in information security with respect to awareness and practice. These specific industry trends were selected because financial institutions expend greater resources on information security than other types of organizations (Kankanhalli et al., 2003). The 2005 Global Security Survey results among member financial institutions reported internal information security breach occurrences (35%) surpassed external security breaches (26%), both of which had risen from prior year statistics (Deloitte Touche Tohmatsu International, 2005). Given the increasing internal and external security breaches, employee awareness and practices were at the bottom of information security priorities among the world's top 100 global financial institutions. However, the lack of employee awareness was perceived as a top information security challenge among half (48%) the member respondents. These current findings were also aligned with reported future information security investment plans, where more resources were targeted for information security tools (64%) and fewer resources were targeted for employee information security awareness (15%). With respect to customer information security awareness, a few reporting member institutions had future plans for customer awareness initiatives.

Research Problem

The boundaries of the formal business computing-environment are no longer well defined because business computer work commonly occurs outside the office (Trouble with homework, 1994). Over 38 million United States workers reside in small office/home office (SOHO) computing-environments, and the numbers are increasing (Wattell, 2002). Employees prefer telecommuting when compared to traditional office work schedules (Tunyaplin, Lunce, and Maniam, 1998). Thus business work occurs in informal computing-environments, where information security threats (Weber, 1988; Rainer et al., 1991; Loch, Carr, and Warkentin, 1992; Fink, 1995; Kearvell-White, 1996; Ryan and Bordoloi, 1997) exist outside the secured boundaries of formal business-computing. Also, converging information technologies allow computing-environments to merge. Broadband connectivity transforms the SOHO and the family computer into Internet nodes. Internet computing introduces additional, dynamic information security threats to formal and informal computing-environments (Rose, Khoo, and Straub, 1999; Hawkins, Yen, and Chou, 2000; Ghosh and Swaminatha, 2001; Hulme, 2001a; Verton, 2002; Knapp, Morris, Rainer, and Byrd, 2003; Schou, 2004). Therefore, informal SOHO and family computing-environments have similar needs for information security as does the formal business computing-environment.

The need for information security enjoys widespread exposure across formal and informal environments. As an example of widespread exposure, a television advertisement for popular virus protection software depicts the folly associated with an elementary-age child surfing the Web through his father's work computer, downloading any software or program that appears enticing. As another example, marketing-savvy Internet Service Providers (e.g. America On-line® or Earthlink®) advertise increased information security at the click-of-a-button. Lastly, the news media frequently updates viewers, listeners, or readers with reports on information security breaches from computer viruses, worms, or hacking incidents. These scenarios appear superficial, which is part of the research problem. With as much exposure, it would seem reasonable to expect that the awareness and practice of information security were well understood. However, this does not appear to be the case.

Purpose of the Study

This research represents the first attempt in establishing an instrument to measure user-level information security awareness through the development of an empirically valid and reliable scale. In its execution, this study represents an initial work in information security research for developing a systematic technique for collecting, analyzing, and interpreting data about information security, and the awareness and practice of information security between formal and informal computing-environments.

This study is significant for several reasons. First, the inability to adequately assess the extent of user-level information security awareness among organizational computer users will hamper future development toward understanding which security practice reflects current trends in information security awareness. Second, the advancement of knowledge about the topic of information security awareness is especially important given the disruptive nature of information technology with respect to information security. Third, an understanding of user-level information security awareness is paramount to top management, whose organizations adopt security practices for three primary purposes: 1) to control costs by reducing risk associated with the loss of business information, 2) align business objectives with information security standards, and 3) to ensure the sustainability of the organization. Fourth, the topic is timely. There is no consensus definition for information security awareness. Furthermore, there is no adequate measure to assess the extent to which user-level information security awareness takes place between computing-environments.

This research aims to fill a void in information security research with respect to the empirical definition of user-level information security awareness. Critical to the evolution of information security research is the development of better user-level awareness measures for variables with which practitioners and researchers rely. Development of measures for the awareness and practice of information security help practitioners and researchers gain experience with valid and reliable measurement. The experience gained can result in 1) a greater understanding of information security and user-level awareness and practice of information security, 2) the identification of variables that are components of user-level awareness and practice of information security, and 3) the realization that user-level information security awareness represents a sound measure of information security practice and ultimately information security.

Scope of the Study

This research is the first step in a larger scheme of inquiry on information security. The ultimate goal of this research is to achieve well-defined, valid, and reliable measurement instruments that assess the variables of interest associated with the awareness and practice of organizational information security. Due to the amount of work and length of time required to complete the overall research scheme, this dissertation focused on user-level awareness and practice of information security. The methodology required for this research involved reporting the results of a content analysis and instrument development effort that hinged on the development of a comprehensive research model that reflects user-level information security awareness among practice in both formal and informal computing-environments. The major components of this dissertation are designed to 1) yield a better understanding of the awareness and practice of information security, and/or 2) establish a sound methodological basis for further study.

Organization of the Dissertation

This dissertation is organized as follows. Chapter I introduces the topic, as well as the need and importance for the research. Chapter II contains a review of the information security literature and the research model from which to develop an individual information security awareness scale. This chapter includes a brief history of disruptive information technologies with respect to information security, an assessment of previous information security research studies, and an examination of the literature relevant to this study. Chapter II concludes with the presented research questions, research hypotheses, and research model. Chapter III presents the research methodology for the study and describes the purpose and procedures for each methodological phase. Chapter IV presents the results of this research. Chapter IV includes the user-level awareness measurement instrument developed, the domain of user-level information security awareness, and data analyses that profile and model user-level information security awareness between formal and informal environments. Chapter V reviews and discusses the research, presents the conclusions from this study, identifies study limitations and implications, and offers recommendations for further research.

CHAPTER II. LITERATURE REVIEW AND RESEARCH MODEL

Introduction

This chapter reviews the previous research on information security, and the awareness and practice of information security. The review found that the literature has not quantified information security trends, nor compared formal, structured (e.g. business) with informal, unstructured (e.g. home) environments.

The chapter opens with a review of information technology (IT) innovations, which affect computer security. The complex computer security domain justifies a review of information security perspectives, models, and definitions. The impact of IT governance and corporate culture on information security also warrants an overview to distinguish information security obedience from awareness. A review of the literature on information security effectiveness follows, which justifies the need for further discussion concerning information security awareness and the trends in information security practice.

The chapter also discusses individual user traits that influence computer practice and ultimately information security. The chapter concludes with a brief summary of the literature presented, and a proposed information security awareness and practice research agenda.

Disruptive Innovations

IT innovations encourage and increase information systems utility (Swanson, 1994). However, innovations can also disrupt organizations by destroying existing competencies (Schumpeter, 1934). IT innovations are disruptive when radical shifts in focus, capabilities, or solutions demand additional IT investment (Friedman and Cornford, 1989). Hulme (2001a, 2001b) and Wattel (2002) noted that IS security requires additional IT investment.

Modern information systems (IS) include five main components: computer hardware, software, data, procedures, and people (Silver, Markus, and Beath, 1995). The importance of modern IS necessitates securing these components from possible threats or vulnerability. Schneier (2002) defined general computer security as the detection and/or prevention of unauthorized actions within and/or to a computer. So, using the premise that IS security began with computer security (Whitman and Mattord, 2005), we can begin with computer threats as a basis for identifying threats to IS security and ultimately information security.

Specific computer security threats and applicable countermeasures result from the following disruptive IT innovations: standalone computing, multi-user computing, personal computers, networks, client/server technology, and Internet computing (Thomson and von Solms, 1998; Lyytinen and Rose, 2003). The following sections review these IT innovations.

Standalone Computing

The term standalone computing refers to early mainframe computers frequently requiring a separate building to meet environmental needs (Schaeffer, 1987). All information input, processing, and output occurred in one secure location. Physical security countermeasures minimized the security threats to standalone computing. Examples of these countermeasures are disaster recovery planning, restricted building access, and environmental controls.

Multi-user Computing

Multi-user computing enabled multiple application processing, multiple user access, and shared system devices (Shelley, Cashman, Waggoner, and Waggoner, 1992). Computer terminals were located in work environments or in home environments via modem access to mainframe connections. These terminals allowed distributed access to trained users, yet all information processing still resided on the mainframe.

Physical security threats continued to exist. However, distributed access requires verifying trusted user identity, which posed a new IS vulnerability. Formal use policy and user authentication address this security threat (Smith, 1987). Formal use policy directs unique user identification assignment, user password format, and user access rights. User identification and a user-specified password combine to form a unique, confidential response. User authentication software challenges trusted users to supply the response. An incorrect response blocks IS entry, while a correct response allows IS entry.

Personal Computers

Personal computers (PCs) moved information processing outside of the secure mainframe environment (Thomson and von Solms, 1998). PCs also introduced a new end-user computing-environment due to proliferation from decreasing prices and expanding capabilities. End-user computing expanded the user link between business and home computing-environments.

White and Christy (1987) noted PCs and end-user computing as potential security control threats. Knowledge, gained through developing IS within end-user computing-environments, affords users the capabilities to circumvent security measures and exploit known security deficiencies. PCs also lacked the necessary operating system controls to restrict access to their resources (e.g. disk drives, computer memory, video display, printers, etc.). As a result, PCs required countermeasures for access control (Boockholdt, 1989).

Unsecured information processing and malicious software are security threats, which require different countermeasures for access control. For example, a PC can process and store sensitive corporate information. A control policy provides security procedures to ensure the integrity of information resources within the business environment (White and Christy, 1987). In a different example, users execute software code to perform desired activities that legally access PC resources. Malicious software code can appear to users as normal software. However, malicious code threatens PC access because undesired activities can result from its illegal resource access. Users execute virus protection software to search memory and drives, identify known malicious code patterns, and remove it (Schneier, 2002).

Networks

Network innovations (e.g. IT infrastructure, network devices, standardized protocols, and standardized software) increased connectivity among computers and networks, in both business and home computing-environments. Increased network use, as an essential tool, builds value (Knapp, Morris, Rainer, and Byrd, 2003). However, increases in network connectivity, complexity, and reliability also increase potential security threats (Thomson and von Solms, 1998). Network data is vulnerable to unauthorized interception and use. As a result, a network requires increases in physical protection, authentication, and access control countermeasures.

Encryption offers a viable countermeasure. Encryption allows scrambling of data during storage or transmission. Encrypted data transmissions or files restrict use to authorized receivers with a decipher key to unscramble or decrypt the data. Key complexity (i.e. length and character content) minimizes the possibility of unauthorized decryption (Schneier, 2002).

Client/sever Technology

Client/server technology (C/ST) offers user participation and expands distributed information processing (Diamond, 1995). Distributed processing allows application-workload sharing between clients (i.e. PCs) and servers (i.e. host computers) over a network (Ryan and Bordoloi, 1997). Shared processing requires different software layers, with each layer requiring frequent, consistent version updates or release patches for functionality. Servers, including mainframes, share processing capability or specialize by function (i.e. application server, file server, print server, web server, etc.).

Fat clients, having greater processing capabilities, yield greater security threats. In contrast, thin clients with limited processing capabilities can limit these potential security threats.

C/ST expands the requirements for authentication, access control, and encryption countermeasures over all network nodes—servers, clients, and network devices. C/ST can considerably increase IT maintenance, which can tax the limits of IT staff resources (Diamond, 1995). However, viable security management countermeasures are policy and procedures, maintained by the IT staff as user-level software guidelines (Schlarman, 2002). C/ST offers flexibility through redundancy and scalability to decrease the impact of physical security threats.

Internet Computing

Lyytinen and Rose (2003) suggested that Internet computing requires the following minimum criteria: the use of n-tier server architecture, a middleware layer, and a thin-client-like browser or wireless application protocol (WAP) phone operating over a transmission control protocol/Internet protocol (TCP/IP) network using hyper-text transfer protocol (HTTP) or other higher level protocols. Figure 1 illustrates these criteria. These criteria also exist as intranets from within known computing-environments and extranets among different known and controlled computing-environments. Internet computing also incorporates previous IT innovations (i.e. multi-user computing, PCs, networks, and C/ST).

Internet computing approaches ubiquitous computing. Banavar and Bernstein (2004) defined ubiquitous computing as embedded within a user's physical computing-environment to seamlessly integrate the migration of data to unknown applications, through unknown environments, to unknown devices, on a global scale. The ubiquitous computing-environment is extremely complex. Schneier (2002) noted that complexity is the worst enemy of security—as IS get more complex, they necessarily get less secure.

Internet Computing Minimum Criteria
(Lyytinen and Rose, 2003)

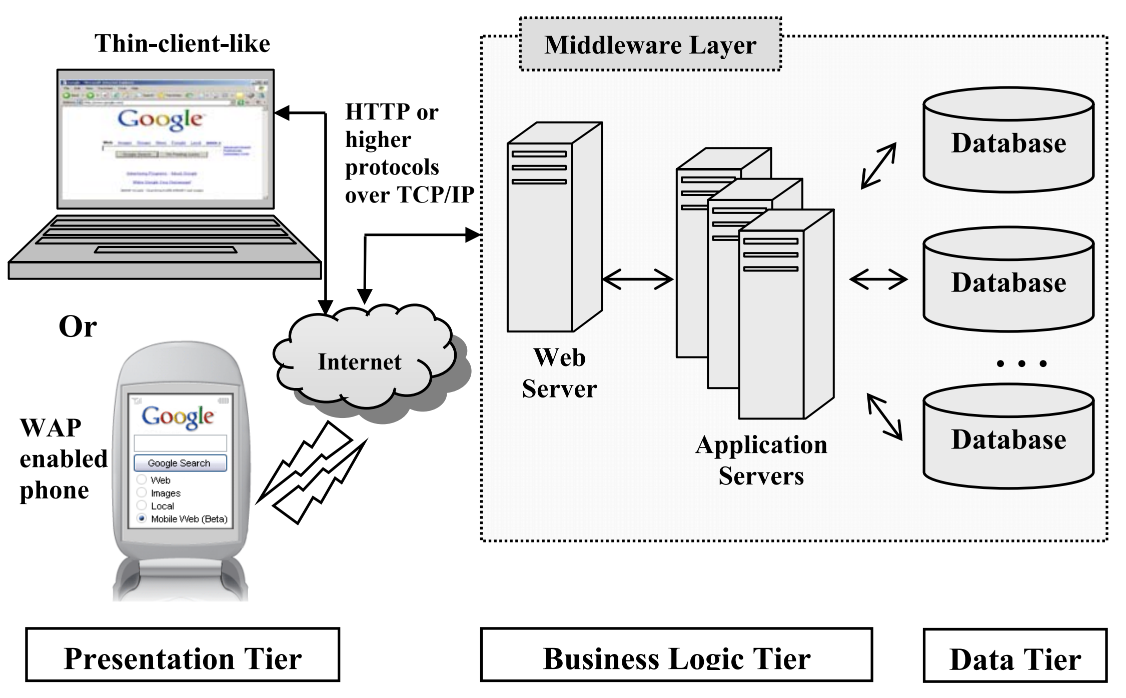


Figure 1

Internet computing changes security domains and expands security perimeters (Hawkins, Yen, and Chou, 2000; Whitman and Mattford, 2005). Just having an Internet connection poses security threats to business and home computing-environments (Ma and Pearson, 2005). Each user-initiated request or reply, over the Internet, can yield a possible security threat (Hawkins et al., 2000).

Ferrarini (2001) suggested security by multiple countermeasures among: physical security, user authentication, access control, encryption, and security management. Internet computing requires both maintenance as well as decision-making for security management countermeasures. Individual user-level security awareness during decision-making ensures proper configuration and functionality of security practices (Hawkins et al, 2000). Schneier (2002) described security as defense in depth, where user awareness of possible security threats equates to multiple, readily available, and applicable countermeasures.

Information Security

Horton (1985) considered IS a business resource with value created in its utility. Information security protects IS utility. However, IT innovations can disrupt information security leaving IS utility vulnerable or at risk. Heiser (2004) viewed information security as an operational risk that is growing in importance, yet managed in a relatively immature way. Straub and Welke (1998) noted that securing IS utility against all threats and dangers is not feasible. Therefore, systems risk is the likelihood that certain threats or loss will affect insufficiently protected IS.

The literature on systems risk has taken different approaches with focus on IT (Rainer, Snyder, and Carr, 1991), IS (Smith, McKeen, and Staples, 2001), electronic commerce (Ghosh and Swaminatha, 2001; Radcliff, 2001), and computing practices (Aytes and Connolly, 2004). However, throughout the literature a common theme in systems risk suggests that only one absolute exists—the lack of security for identified and unidentified threats will increase systems risk.

Evaluating systems risk identifies potential threats or existing vulnerabilities, and then evaluates the trade-offs between the identifiable threats, costs of countermeasures, and the potential loss of value (Rainer et al., 1991; Smith et al., 2001). Smith et al.

(2001) proposed that systems risk can focus on one of its components, or information risk. To that end, information risk is a trade-off between the costs of countermeasures for potential threats against the combined value of potential loss. Smith et al. (2001) noted the growing recognition that information risk cuts across all organizational levels (e.g. strategic, tactical, or operational) for management and control. The authors also suggested that the integrated management of systems risk should be an ongoing process that requires identification, assessment, and action for all IS components.

This dissertation defines information security as continuous deterrent and preventive efforts, which have the behavioral intent to secure or limit the loss in IS utility. These continuous deterrent and preventive efforts are derived and accomplished through the identification of possible security threats, assessment of the associated information risk or cost to loss ratio, decision to mitigate the associated information risk, and employment of appropriate, associated security countermeasures. A closer review of deterrent and preventive efforts, information security models, and a security classification scheme follows.

Deterrent and Preventive Efforts

The literature notes the importance of deterrent and preventive efforts for security (Martin, 1973; Madnick, 1978; Weber, 1988; Straub, 1990; Straub and Nance, 1990; Forcht, 1994; Gopal and Sanders, 1997; Straub and Welke, 1998; Hawkins et al., 2000; Kankanhalli, Teo, Tan, and Wei, 2003; Leach, 2003; Eaton, 2004; Stanton, Stam, Mastrangelo, and Jolton, 2005). Straub (1990) and Kankanhalli, et al. (2003) suggested that both deterrent efforts and preventive efforts have positive influence on IS security effectiveness. However, deterrent efforts and preventive efforts provide different approaches for information security.

While deterrent and preventive efforts are both proactive, Straub and Nance (1990) noted that deterrent efforts are passive and preventive efforts are active. Deterrent security efforts take the form of policies, procedures, or guidelines to lower information security risk by defining acceptable use (Klete, 1978; Parker, 1981; Dunn, 1982; Parker, 1983; Straub 1990; Forcht, 1994; Kankanhalli, Teo, Tan, and Wei, 2003; Schwartz, 2004). Policies, procedures, or guidelines attempt to persuade users to adhere to specific security behavior patterns. However, users may not choose to comply. Preventive security efforts limit information security risk through specific controls (Hsaio, Kerr, and Madnick, 1978; Weber, 1988; Forcht, 1994; Kankanhalli, Teo, Tan, and Wei; 2003). Preventive efforts such as door locks, separate thermostats, or specific software (i.e. firewalls, virus protection, authentication, or email filters) attempt to actively control a specific IS security threat. However, a preventive effort does not provide absolute security against a specific IS threat. Locks have keys, thermostats adjust, or users may choose to bypass software control.

Deterrent and preventive security efforts are also complementary. Combined deterrent and preventive efforts reduce IS vulnerabilities and information security threats (Straub, 1990; Kankanhalli et al., 2003). Preventive efforts such as physical security or security software constitute additional layers of security countermeasures when deterrent efforts are ineffective (Straub and Welke, 1998). For example, a restricted entry policy for computer facilities may deter some users, yet a door lock should limit entry to all users without a key. As a different example, an acceptable network use policy may deter some users from browsing the Internet, yet network firewall software can block the specific TCP/IP port used for HTTP. Hence, preventive efforts can enforce deterrent efforts (Gopal and Sanders, 1997). Deterrent efforts can also enforce preventive efforts such as a corporate virus protection policy that requires the use of specific virus protection software on all network computers.

Deterrent and preventive security efforts are concerned with the characteristics of confidentiality, integrity, and availability. Whitman and Mattord (2005) referred to these three characteristics as the C.I.A. triangle and Schneier (2002) called them the traditional three pillars of computer security. These three information characteristics, through the application of deterrent or preventive efforts, provide the basis for information security.

Confidentiality. Schneier (2002) noted that the bulk of military-funded computer research has centered on confidentiality, with an industry bias toward this characteristic in most computer-security products. Schneier pointed out that confidentiality in the context of computer security meant read access. However, confidentiality does not imply privacy because privacy is a security need rather than a characteristic of information (Smith, McKeen, and Staples, 2001; Schneier, 2002).

Whitman and Mattord (2004) suggested that confidentiality required only authorized users with sufficient privileges and a demonstrated need to access certain information. Confidentiality requires a demonstrated or sufficient need to access sensitive information, in addition to sufficient privileges for read access. An illustration of the confidentiality characteristic would be a bank teller and account balances. A bank teller has sufficient access privileges to read account balances, but confidentiality dictates that the teller can only access and read an account balance in response to a request from the account owner. Therefore, confidentiality deals with read access to sensitive information.

Thompson and Kaarst-Brown (2005) noted the dilemmas associated with users identifying sensitive information and interpreting its required level of confidentiality. The authors proposed research methodology to address the complexity of an individual's interpretation of sensitive information. They suggested that economic, legal, social, and psychological knowledge domains frame the context of understanding sensitive information classifications. However, classification schemes for sensitive information require forethought because individuals who develop sensitive information classification schemes may not be the user(s) who interpret individual information sensitivity. Information security countermeasures should differentiate the necessary read access to protect sensitive information and provide confidentiality. The authors also suggested that to understand how individuals in an organization interpret sensitive information, research is required to capture thinking (awareness) at an individual level within the context of the organization. The same approach can apply to capture and interpret confidentiality, or information security, in the context of the organization.

Integrity. Irvine and Levin (2002) noted the critical nature of information integrity. Information integrity is the lack of exposure to accidental or malicious alteration or destruction. As a result, information with integrity is reliable as the basis for critical decisions. Whitman and Mattord (2004) emphasized that corruption or access control threats to information integrity can occur during entry, storage, or transmission. Nayar (2002) summarized integrity as the dependability or trustworthiness of information where it represents accuracy, consistency, and reliability of the information content, process, and system. Schneier (2002) suggested that integrity was the most difficult of the three characteristics to define, especially with the advent of Internet computing. Schneier also offered his definition of information integrity as “every piece of data was as the last authorized modifier left it” (p. 122).

The characteristic of integrity constrains write access (Schneier, 2002). Schneier stated that a computer virus breaches information integrity because a virus can maliciously corrupt information via unauthorized write access. Information security practices against computer virus corruption would include access control countermeasures via deterrent efforts from policies or guidelines along with preventive efforts from anti-virus software.

Irvine and Levin (2002) also provided mathematical proof that exposure of information within IS, or IS components, having lower information integrity capacity will limit information integrity. Their results suggested that IS, where C/ST is composed of a high-integrity client (e.g. web browser) and server components that encrypt communications to prevent exposure during transmission through low-integrity network components, could provide high integrity information. Encryption countermeasure examples of this scenario are a virtual-private-network (VPN) connection, a secure socket layer connection for e-commerce transactions, secure electronic transactions (SET) as developed by commercial credit card companies, secure hyper-text transfer protocol (HTTPS), or secure shell (SSH) developed for secure remote access connections between a client and server.

Integrity is also the basis for data quality. Through integrity, data quality can consequently create added value in data entry, storage, and processing as demonstrated in electronic data interchange, electronic commerce, supplier resource management, customer resource management, and the supply chain. Nayar (2002) noted that information integrity can eliminate batch processing cycles within IS to produce a zero latency or real-time business computing-environment. Customer orders or supplier invoices are automatically processed when presented to the IS, without human verification or intervention beyond the source data-entry from the customer or supplier. Strous (2002) also noted that added value through data quality was a more appealing approach in justifying information security to top management through information integrity.

Availability. Whitman and Mattord (2004) described availability as the characteristic of information that enables an authenticated user (i.e. defined as a person or computer) to access information without interference or obstruction and in a useable format. Schneier (2002) defined availability as ensuring that an attacker cannot prevent legitimate users from having reasonable access to IS (e.g. denial-of-service attacks). In general, users of IS expect information to be available when they expect it and as they expect it. Therefore, availability requires physical, authentication, access control, encryption, and security management countermeasures against security threats.

Wattel (2002) suggested that information availability to authenticated users should occur through security policy enforcement (e.g. deterrent efforts) and software constraints (e.g. preventive efforts) within the individual critical business process. For example, if a given user attempts to open a database file without Microsoft Access when the security policy states that Microsoft Access is the only option, then the user cannot open the database. As another example, if an authorized user attempts to email a sensitive document unencrypted when policy dictates encryption, then the process halts and the specific policy with an explanation why the rule was important appears in a decision window. If the user agrees to encrypt the document, then the document encryption occurs and the email follows. Successful execution of the business process mandates security policy compliance, achieving security policy obedience, and information security awareness. When security policy directs information availability, the policies are effective and user education can occur.

Information Security Models

Both the public and private sectors have recognized the complexity of information security in regards to human and technology factors. Ma and Pearson (2005) noted that the adoption of existing models or frameworks could expedite the methodology for implementing information security. Whitman and Mattord (2005) described such an approach as information security blueprints. The literature provides information security models with origins from international standards, government agencies, and the United States Department of Defense. These models or blueprints provide the basis for information security deterrent efforts through security policy and IT governance.

International standards. Published in 1995, The British Standard BS 7799 builds on earlier Department of Trade & Industry codes of practice (Kearvell-White, 1996). Whitman and Mattord (2005) described BS 7799 as one of the most widely referenced security models. The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) adopted BS 7799 in 2000 as ISO/IEC

17799. British Standard BS 7799:2 also later extended ISO/IEC 17799 with information on its suggested implementation.

Ma and Pearson (2005) empirically validated seven of the ten constructs from guidelines and practices within ISO 17799, and consequently IEC 17799 and BS 7799. Table 1 lists the ISO 17799 constructs and notes the seven validated constructs. Unfortunately, as with ISO compliance certification and verification, the details of ISO/IEC 17799 are available only through the purchase of the standard and only businesses operating in the European Union are obligated to comply (Whitman and Mattord, 2005).

Constructs for Information Security Practices from ISO 17799

(Ma and Person, 2005)

Construct	Items	Coefficient Alpha
Information Security Policy*	6	.93
Organizational Security*	6	.88
Asset Classification & Control*	4	.85
Business Continuity Planning*	4	.92
System Access Control*	8	.86
System Development & Maintenance*	5	.89
Communications & Operations Management*	11	.91
Physical & Environmental Security **	4	.81
Personnel Security **	5	.83
Compliance **	3	.83

* Validated construct

** Construct items either did not load (did not exceed 0.5) or loaded on other dimensions

Table 1

Government agencies. The Computer Security Resource Center of the National Institute for Standards and Technology (NIST) offers assistance in the design of security frameworks. The United States government, when deciding not to select the ISO/IEC 17799 standards, cited the NIST references. NIST documents are publicly available at no charge as possible best practices for information security blueprints. With respect to information security, government and industry professionals have broadly reviewed the NIST publications. Whitman and Mattord (2005) cited the following documents as framework references:

- SP 800-12: *Computer Security Handbook*
- SP 800-14: *Generally Accepted Security Principles & Practices*
- SP 800-18: *Guide for Developing Security Plans*
- SP 800-26: *Security Self-Assessment Guide for Information Technology Systems*
- SP 800-30: *Risk Management for Information Technology Systems*

In addition to these references, *NIST Special Publication 800-53* was issued with respect to recommended guidance for security controls within IS of federal agencies (Ross, Katzke, Johnson, Swanson, Stoneburner, Rogers, and Lee, 2005).

The Committee on National Security Systems (CNSS), formerly known as the National Security Telecommunications and Information Systems Security Committee (NSTISSC), published NSTISSI No. 4011 as a flexible, comprehensive model of information security. Acknowledging its rapid acceptance and potential, Whitman and Mattord (2004) recognized the NSTISSI model as a standard for IS security and a definition of information security. The NSTISSC security model uses a three-dimensional matrix framework to evaluate information security based on 27 intersecting relationships among: dimension one—confidentiality, integrity, and availability; dimension two—storage, processing, and transmission; and dimension three—policy, education, and training.

The NSTISSI model provides a framework to identify potential gaps in information security, yet it does not provide suggestions with respect to deterrent efforts from policies and guidelines.

Department of Defense. The United States Department of Defense has funded many information security models (Schneier, 2002). These models were developed to formalize IS utility according to a sensitive information classification scheme and tended to model confidentiality, with the most notable being the Bell-LaPadula model. Schneier also noted that the Bell-Lapadula model failed to offer useful and cost-effective information security, yet its theory has had a lasting impact on IS security design.

Five-Access Point Security Classification

Schneier (2002) viewed computer security as a continual process. Ferrarini (2001) proposed a similar continual process approach to network security, and consequently to computer and information security, by minimizing possible unauthorized entry to each identified network access point. The five access points Ferrarini suggested as candidates for continuous scrutiny and concern against security threats are physical protection, authentication, access control, encryption, and security management.

When developing, implementing, and maintaining information security, these five access points provide a reference classification or scheme that can target appropriate countermeasures. Figure 2 illustrates a layered approach to the five-access point security scheme that provides a consistent scope for classification of information security vulnerabilities across security policies during security threat analysis, security planning, and security contingency planning. Information security vulnerability issues presented under a common classification scheme can provide a coherent basis for information security decisions.

A Layered Approach to a Five-access Point Security Scheme.
(adapted from Ferrarini, 2001)

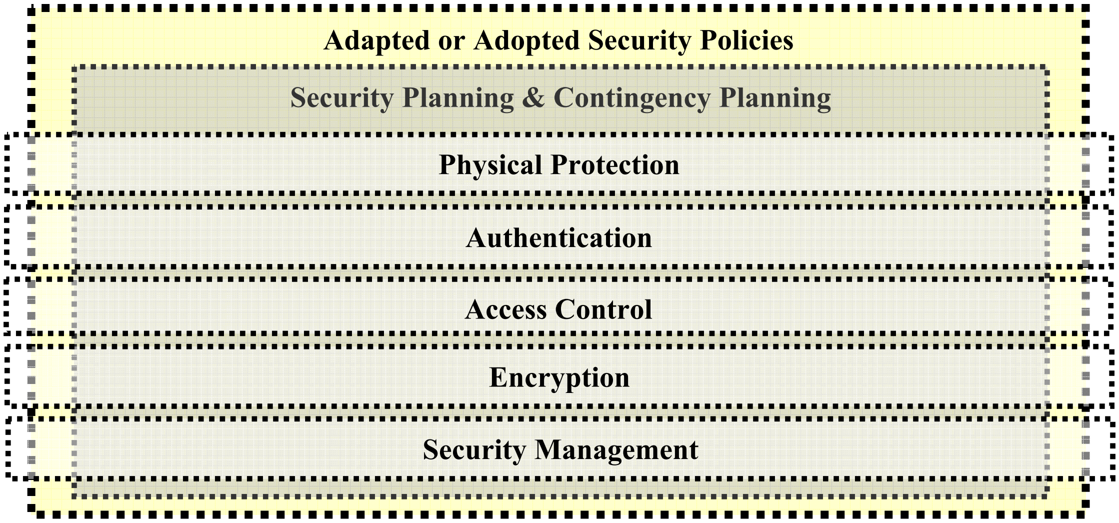

Adapted or Adopted Security Policies
Security Planning & Contingency Planning
Physical Protection
Authentication
Access Control
Encryption
Security Management

Figure 2

Ferrarini (2001) noted that an effective seal on any security access point was dependent on weighing the associated security risk, the cost of implementing the security countermeasure, and the value associated with the consequences of a given security breach. Rainer, Snyder, and Carr (1991) suggested that overall risk posture was a management responsibility. Coherency is desirable when management executes their inherent duty of controlling costs and devising strategy to maximize returns while aligning business objectives with information security standards (Ramanathan, 2004).

Information Security, IT Governance, and Corporate Culture

Formal or informal rules of appropriate behavior can guide individual and group actions, which lead to regularity, structure, and knowledge transfer (Gouldner, 1954;

Weber, 1978; Jackall, 1988; March and Olsen, 1989; Friedkin and Cook, 1990; Frank and Fahrbach, 1990; Zhou, 1993; Dixon, 1998; Ocasio, 1999; Wu and Rocheleau, 2001; Kanter, 2003). Thomson and von Solms (1998, 2005) proposed that information security is a learned behavior. A behavior based on formal and informal sources, which can influence through operational, physical, and technical actions within the computing-environment, along with cognitions, behavioral intentions, attitude, and affective responses of the individual user.

Thomson and von Solms (1998) suggested that user-level information security requires discipline and education to reinforce IS security during day-to-day user activities, especially if day-to-day user activities disregard IS security. Lewis, Agarwal, and Sambamurthy (2003) noted that support of a technology was grounded in individual beliefs about the value of the technology. Also, user-level discipline and education for information security are available via formal (e.g. IT governance) and informal (corporate culture) influences in business organizations (Thomson and von Solms, 2005).

IT Governance

Management dictates IT governance, fundamentally driven by managerial objectives that IT deliver value, have accountability, and have acceptable risks. IT governance extends formal rules from top management's mission of defining strategic direction to ensure that IT objectives are met, IT risks are managed, and IT resources are used responsibly (Guldentops, 2002). Yet, management priorities assigned individually to IS utility and information security (Ball and Harris, 1982; Dickson, Leitheiser, Wetherbe, and Nechis, 1984; Brancheau and Wetherbe, 1987; Niederman, Brancheau, and

Wetherbe, 1991; Brancheau, Janz, and Wetherbe, 1996) do not reflect an urgency to manage IT risk.

The lack of urgency could imply a lack of management's information security awareness. It could also suggest a lack of management priority to address information security risk. In either case, recent government regulations concerning information security (e.g. Huston, 2001; Heiser, 2004; Loeber, 2004; Ramanathan, 2004) call for additional IT governance through information security awareness or obedience to the regulations (i.e. policies). Either case would contribute to the growing recognition of information security risk as claimed by Smith et al. (2001). Heiser (2004) also noted that foreign regulations preceded domestic regulations, which could also explain the gap found between domestic and international management priority for information security (Watson, Kelly, Galliers, and Brancheau, 1997).

IT governance arrangements direct, control, and coordinate the day-to-day delivery of IT operations and services (Sambamurthy and Zmud, 1999). As part of these arrangements, Whitman and Mattford (2005) suggested that an information security policy should provide rules for the protection of information assets that support the organization's mission/strategy and shape the philosophy of security in the IT environment. Whitman and Mattord (2004) noted that information security expertise acquired through day-to-day IS involvement is an advantage to IT governance. Therefore, IT governance arrangements should employ cross-functional team reviews of security policy options and implementation.

As a deterrent effort, a security policy should also provide a framework for selecting and implementing consistent countermeasures against information security threats

(Schneier, 2002). Stephen Northcutt, director of training and certifications with the SANS institute, stated that a security policy should guide users' actions—empowering a user to do the right thing as the main goal (Schwartz, 2004). Ultimately the security policy determines which countermeasure(s) to use. In the absence of such policy, Schneier (2002) noted that individual users could generate inconsistent countermeasures based on their own individual levels of information security awareness, which in the aggregate could yield an inconsistent, incoherent, or ineffective information security policy.

Corporate Culture

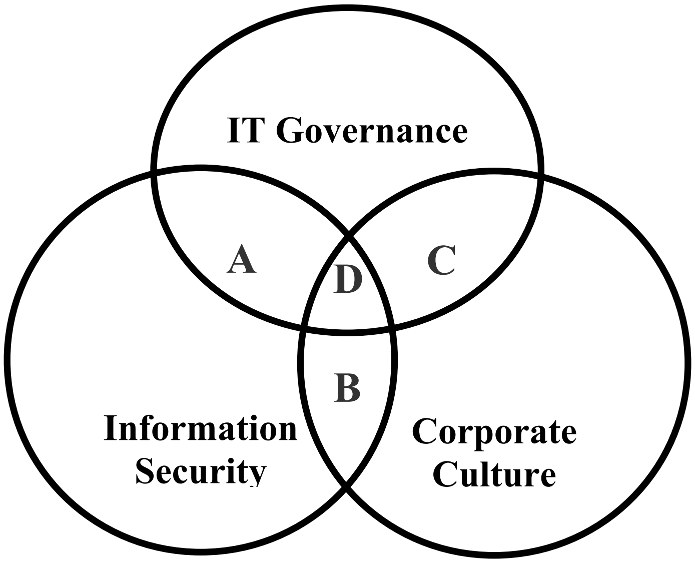
Corporate culture represents the informal rules of appropriate behavior dictated by individuals who do the actual work (Hofstede, 1984). Schein (1985) stated that culture is "a pattern of basic assumptions—invented, discovered, or developed by a given group as it learns to cope with problems of external adaptation and internal integration—that have worked well enough to be considered valid and, therefore, to be taught to new members as the correct way to perceive, think, and feel in relation to those problems" (p. 9).

Ultimately, sense-making efforts and actions of individuals manifest, represent, and maintain corporate culture (Harris, 1994). Mutually learned values, beliefs, and assumptions that fundamentally drive corporate culture become second nature to the individual member (Schein, 1999). These learned norms have a direct influence on the day-to-day behavioral patterns of individual members within computing-environments (Wu and Rocheleau, 2001; Gillespie and Nakatomi, 2002). Therefore, corporate culture can affect information security because corporate culture affects individual user practice (i.e. deterrent security efforts and/or preventive security efforts).

Conceptual Relationships with Information Security

Thomson and von Solms (2005) proposed conceptual relationships among information security, IT governance, and corporate culture (see Figure 3). These relationships are relevant because effective IT governance and supportive corporate culture that both encourage desirable information security practice should positively influence information security. Thomson and von Solms also proposed the concept of information security obedience, depicted as relationship D in Figure 3.

Information Security, IT Governance, and Corporate Culture
(Thomson and von Solms, 2005)



A – The relationship that should exist between IT governance and information security.
B – The relationship between information security and corporate culture.
C – The relationship between IT governance and corporate culture.
D – The relationship between IT governance, corporate culture, and information security.

Figure 3

Information security obedience is user behavior complying with the vision of IT governance to meet information security requirements (Thomson and von Solms, 2005). Unfortunately, obedience masks awareness because obedience implies user compliance to information security policy while awareness implies user knowledge or understanding about the need for information security. Information security decision-making requires awareness more so than obedience.

Leach (2003) noted that as information security decisions continue to increase in day-to-day user activities, improvement in security decision-making skills strengthen user security behavior. Similarly, Stanton, Stam, Mastrangelo, and Jolton (2005) suggested that small increases in user-level security awareness could shift improvement in user security behavior from naïve mistakes toward basic security hygiene. A research agenda for the awareness and practice of information security should differentiate information security obedience from information security awareness.

Effective Information Security

An increase in information security awareness is a recurrent theme in the literature (Madnick, 1978; Straub, 1990; Kankanhalli, Teo, Tan, and Wei, 2003; Egan 2004). As former Chief Information Officer at Symantec Corporation and author of *The Executive Guide to Information Security*, Mark Egan (2004) offers ten traits of effective information security that he considers essential (refer to Table 2).

Straub (1990) and Kankanhalli et al. (2003) empirically tested theoretical models for effective IS security that included many of the traits listed in Table 2. Both studies, as well as practitioners (Spurling, 1995; Hulme, 2001a; Egan, 2004; Ramanathan, 2004), call for user-level information security awareness across the entire organization to sustain effective IS security.

Ten traits of effective information security.

(Egan, 2004)

1. Information security is regarded as an essential business investment.
2. The CEO or COO owns information security.
3. Information security starts with the basics.
4. Senior level staff has responsibility for information security.
5. The IT governance board is comprised of a cross-functional team.
6. Multi-layered security is in place.
7. Zones divide the computing-environment.
8. Information security is measurable.
9. Information security is not static.
10. Information security is audited by an independent third-party.

Table 2

Straub (1990)

Straub examined the IS security literature for the period 1967 to 1988, finding evidence that IS security was a low management priority with correspondingly low levels of IS security investment. The study employed the criminological theory of general deterrence to justify IS security efforts and encourage increased management investment in IS security. The results supported constructs for deterrent efforts (certainty and severity) and preventive efforts (security software) to explain losses from computer abuse incidents. Figure 4 illustrates the model and Table 3 defines the constructs.

Straub's results stated that both IS staff deterrent efforts and preventive security software efforts negatively influenced computer abuse. Straub concluded that effective IS security uses deterrent and preventive efforts to reduce losses from computer abuse incidents. Straub suggested the establishment of detailed security policies regarding proper and improper IS use, along with multiple methods to inform and educate users on the resultant security policies. Straub also suggested that management consider the implementation of preventive security software.

The Security Impact Model
(Straub, 1990)

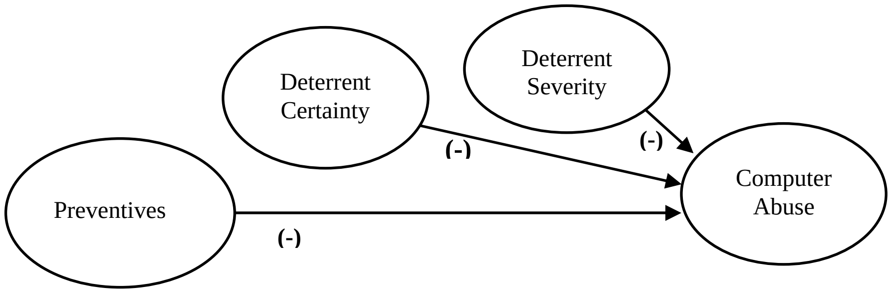


Figure 4

The Security Impact Model: Concepts, Constructs, and Measures
(Straub, 1990)

Concepts	Constructs	Measure Description
Computer Abuse	Computer Abuse	▪ Number of computer abuse incidents ▪ Actual dollar loss ▪ Opportunity dollar loss ▪ Subjective computer abuse seriousness index
Deterrents	Deterrent Certainty	▪ Number of full-time security staff ▪ Number of part-time security staff ▪ Total security hours per week ▪ Data security hours per week ▪ Total security staff salaries ▪ Subjective estimate of deterrent security effect ▪ Age of IS security program (elapsed time from program inception to computer abuse incident)
	Deterrent Severity	▪ Severity of penalties for computer abuse ▪ Number of informational sources on computer abuse ▪ Subjective estimate of deterrent security effect
Rival Explanations	Preventives	▪ Number of operating system and database management system security software programs ▪ Number of specialized security software programs

Table 3

The impact of deterrent and preventive security efforts from IS users beyond the IT security staff is one of Straub's (1990) main implications. Straub based the deterrent certainty construct on security man-hours expended, yet the study included only IT security staff efforts. The results did not account for the security efforts of other IS users. Increasing user-level information security awareness and the resulting deterrent and preventive efforts should increase the overall security man-hours expended. The effectiveness of IS security based on deterrent and preventive efforts from all IS users should exceed the effectiveness of IS security based on deterrent and preventive efforts from only the IT security staff.

Kankanhalli, Teo, Tan, and Wei (2003)

Kankanhalli, Teo, Tan, and Wei examined the IS security literature for the period 1978 to 2002. The study found evidence that IS security continued to have low management priority with correspondingly low levels of IS security investment. The study employed known IS organizational factors that affect IS implementation to distinguish any associated impacts about IS security measures. The authors' intent was to inform IS management on effective IS security measures and any associated distinguishable organizational factors. The results show that organizational factors (size, top management support, and industry type) and security measures (deterrent efforts and preventive efforts) help explain IS security effectiveness. Figure 5 illustrates the model and Table 4 defines the model constructs.

Integrated Model of IS Security Effectiveness

(Kankanhalli, Teo, Tan, and Wei, 2003)

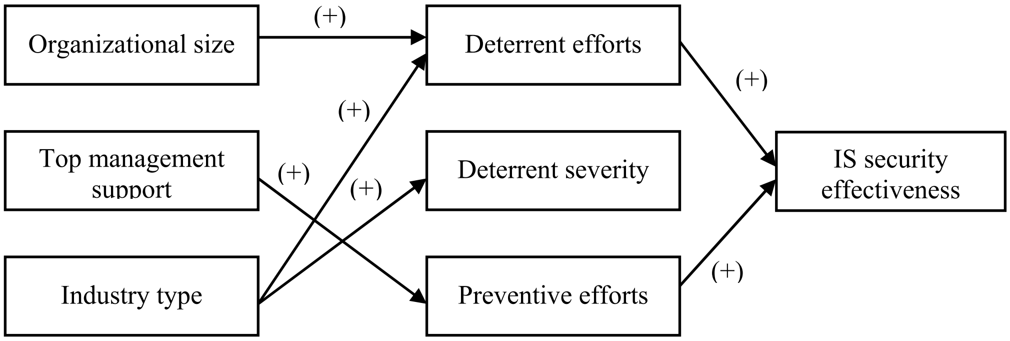


Figure 5

Integrated Model of IS Security Effectiveness: Constructs and Measures

(Kankanhalli, Teo, Tan, and Wei, 2003)

Constructs	**Measure Description**
IS security effectiveness	▪ Overall deterrent effectiveness ▪ Overall preventive effectiveness ▪ Protection of hardware effectiveness ▪ Protection of software effectiveness ▪ Protection of data effectiveness ▪ Protection of computer services effectiveness
Deterrent efforts	▪ Total IS security man-hours expended per week
Deterrent severity	▪ Form of organizational punishment for IS security abuse (no action, reprimand, suspension, dismissal, and prosecution).
Preventive efforts	▪ Number of operating systems with embedded security software ▪ Number of DBMS with embedded security software ▪ Number of specialized security programs
Organizational Size	▪ Number of employees
Top Management Support	▪ Higher management attendance in IS security meetings ▪ Higher management involvement in IS security decisions ▪ Higher management involvement in monitoring IS security activities ▪ Higher management support for IS security functions
Industry Type	▪ Financial organizations versus other organizations

Table 4

Results from the Kankanhalli et al. model supported that only deterrent efforts and preventive efforts contributed to IS security effectiveness. Deterrent severity had no relationship with IS security effectiveness. Since deterrent severity or severe improper IS use penalties had no impact on IS security effectiveness, the authors suggested that organizations should focus security measures on deterrent and preventive efforts. Overall, the study suggested inconsistency or lack of information security awareness among IS managers for deterrent and preventive security efforts. Larger organizations invested more in deterrent efforts than smaller organizations, yet organizational size had no relationship with preventive efforts. Top management support positively related to preventive efforts, yet top management support had no relationship with deterrent efforts. In addition, financial organizations invested more in deterrent efforts than non-financial organizations, yet industry type had no relationship with preventive efforts.

The inconsistency in information security awareness between deterrent efforts (e.g. security man-hours expended per week) and preventive efforts (e.g. level of security software sophistication) among IS managers is an important finding from Kankanhalli et al. (2003). Combined deterrent and preventive efforts provide effective information security. User-level information security awareness should provide consistency in application of both deterrent and preventive efforts.

Top Management Support

The strategic planning impact of business and IT alignment on IS development is well documented in the literature (King, 1988; Madnick and Wang, 1988; Andreu, Ricart, and Valor, 1994; Brown and Magill, 1994; Teo and King, 1997; Ross 2003). Similar experiences in bottom-up versus top-down strategic planning during IS security development may account for the inconsistency in top management impacts on deterrent and preventive efforts. Ramanathan (2004) stated that differing approaches to strategic information security planning (i.e. bottom-up versus top-down) have yielded different levels of success and top management support.

Traditional information security has resulted from bottom-up planning, initiated by employees and IT staff, who present their findings to management as proposed security policy recommendations (Ramanathan, 2004). Top management support is a critical success factor. Unfortunately, bottom-up planning lacks a holistic business focus and top management may not understand the associated information security risk or comprehend the recommendations.

On the other hand, top-down planning requires that executive management investigate and take ownership of security framework models that mitigate information risk. Top management should own information security with senior-level executives having the responsibility for information security (Egan, 2004). This process allows management to execute their duty to control costs and to devise strategy that maximizes returns while aligning business objectives with information security standards (Ramanathan, 2004). Top management support results in the allocation of resources to deploy preventive security efforts (Kankanhalli et al., 2003). Top-down planning calls for top management support that result in the allocation of resources to deploy both preventive and deterrent security efforts.

Whitman and Mattord (2004) noted that bottom-up planning does offer the advantage of expertise, acquired through the day-to-day involvement with IS. The same expertise is also available in top-down planning during cross-functional team reviews of security policy options or as an implementation perspective to fine-tune deterrent efforts and propose optimal preventive efforts. With respect to information security, expertise infers domain knowledge.

The Chief Information Officer (CIO) provides IT expertise in planning the strategic alignment of business and IT objectives (Hawkins et al., 2000). Whitman and Mattord (2004) also suggested the addition of a Chief Information Security Officer (CISO) who could help the CIO with tactical and operational security planning. Reich and Benbasat (2000) suggested that although communication between business and IT executives impact the short-term alignment of business and IT objectives, shared domain knowledge between business and IT executives' impacts long-term alignment. During executive interviews, Cline and Jensen (2004) noted that top managers picked information security awareness as a major issue. Shared awareness is shared domain knowledge or shared expertise. User-level information security awareness across the organization should alert top management to support both deterrent and preventive efforts for effective IS security.

Information Security Awareness

Deterrent and/or preventive efforts result from security decisions. Researchers (Straub, 1990; Hawkins et al., 2000; Furnell, Gennatou, and Dowland, 2002; Kankanhalli et al., 2003; Leach, 2003; Stanton et al., 2005) and practitioners (Spurling, 1995; Hulme, 2001a; Eaton, 2004; Ramanathan, 2004) note the importance of information security awareness during strategic, tactical, and operational security decision-making. Most studies simply call for additional information security awareness through IS security training. However, some studies explore or detail the methodology required in educational programs to raise user-level information security awareness (Spurling, 1995; Thomson and von Solms, 1998; Siponen, 2000, 2001; Leach, 2003; Schou and Trimmer, 2004; Stanton et al., 2005).

Few studies have considered information security awareness in detail (Siponen, 2000, 2001; Furnell et al., 2002; Leach, 2003; Stanton et al., 2005), and fewer studies have considered the establishment of a measurement model of information security awareness (Furnell et al., 2002; Leach, 2003; Stanton et al., 2005). Furnell, Gennatou, and Dowland, (2002) suggested a computer-based training tool prototype for information security awareness in small organizations. Stanton et al. (2005) suggested that small increases in security awareness could shift user authentication behavior from naïve mistakes toward basic security hygiene.

The literature notes the importance of information security awareness based on the domain knowledge of security threats (Thomson and von Solms, 1998, Hawkins et al., 2000; Siponen, 2000; 2001, Furnell, et al., 2002; Leach, 2003; Stanton et al., 2005). Threat-context expertise is an understanding of potential threats to IS utility balanced with the knowledge of appropriate threat countermeasures.

Information Security Threats

The identification of potential security threats is a dynamic process. A threat to information security is any possible action that could compromise IS utility. To that end, many researchers and practitioners have identified and prioritized various information security threats (Weber, 1988; Rainer et al., 1991; Loch, Carr, and Warkentin, 1992; Fink, 1995; Kearvell-White, 1996; Ryan and Bordoloi, 1997; Rose, Khoo, and Straub, 1999; Hawkins et al., 2000; Ghosh and Swaminatha, 2001; Hulme, 2001a; Verton, 2002;

Knapp, Morris, Rainer, and Byrd, 2003; Schou, 2004). Table 5 summarizes these information security threats.

Information Security Threats

Author	Type of Threats Identified
Weber (1988)	Physical
Rainer, Snyder, and Carr (1991)	Physical; unauthorized physical and electronic access; obsolete software; and end-user computing
Loch, Carr, and Warkentin (1992)	MIS executives' ranking of 12 threats by mainframe, microcomputer, and network environments.
Fink (1995)	Top ten future threats perceived by Australian IS management.
Kearvell-White (1996)	Managing data; viruses; access control; passwords; back-up data; and physical survey results with respect to the introduction of British Standard BS 7799.
Ryan and Bordoloi (1997)	Mainframe and client/server
Rose, Khoo, and Straub (1999)	Business-to-consumer (B2C)
Hawkins, Yen, and Chou (2000)	Unauthorized access and network intrusion in Internet computing
Ghosh and Swaminatha (2001)	Mobile and e-commerce
Hulme (2001a)	Large corporation security breach survey results
Verton (2002)	Corporate disaster from terrorist attacks
Knapp, Morris, Rainer, and Byrd (2003)	Network
Schou (2004)	Information Systems Security Certifying Consortium's ten domains of knowledge from which security threats evolve.

Table 5

Weber (1988) identified physical security threats of fire damage, water damage, energy variations, structural damage, pollution, and unauthorized intrusion. Weber noted that information access points are more vulnerable to security threats. Physical entry into the computer building and eavesdropping in the form of wire-tapping comprised the two forms of unauthorized intrusion at the time. Weber discussed an early case of extended security perimeter eavesdropping where data processing outside the computer installation occurred through interceptions of unshielded electromagnetic signals.

In contrast to the physical threats noted by Weber (1988), Schou and Trimmer (2004) recognized the increased complexity of modern IS, the associated complexity in security threats, and the depth of professionalism required to identify these complex security threats. As listed in Table 6, the International Information Systems Security Certifying Consortium (ISC^2) classified ten domains of knowledge that can spawn potential security threats (Schou and Trimmer, 2004). According to the ISC^2, professionals need mastery and users need awareness of the ten domains.

ISC^2 Domains of Knowledge for Potential Security Threats

(Schou and Trimmer, 2004)

1) Access Control Systems & Methodology
2) Applications & Systems Development
3) Business Continuity Planning
4) Cryptography
5) Law, Investigation, & Ethics
6) Operations Security
7) Physical Security
8) Security Architecture & Models
9) Security Management Practices
10) Telecommunications, Network, & Internet Security

Table 6

Depth of Expertise

Siponen (2000) suggested that every computing-environment comprises various user-level depths or stages of information security awareness (e.g. threat-context expertise). Schou and Trimmer (2004) noted a similar learning hierarchy applicable to information security based on the NIST Standard 800-16 and the CNSS standards 4011 through 4016. Applying this hierarchy IS users follow a staged progression from computer literacy, to information security awareness, to information security practice, and ending with information security education.

Threat-context Expertise and Security Decisions

(adapted from Schou and Trimmer, 2004)

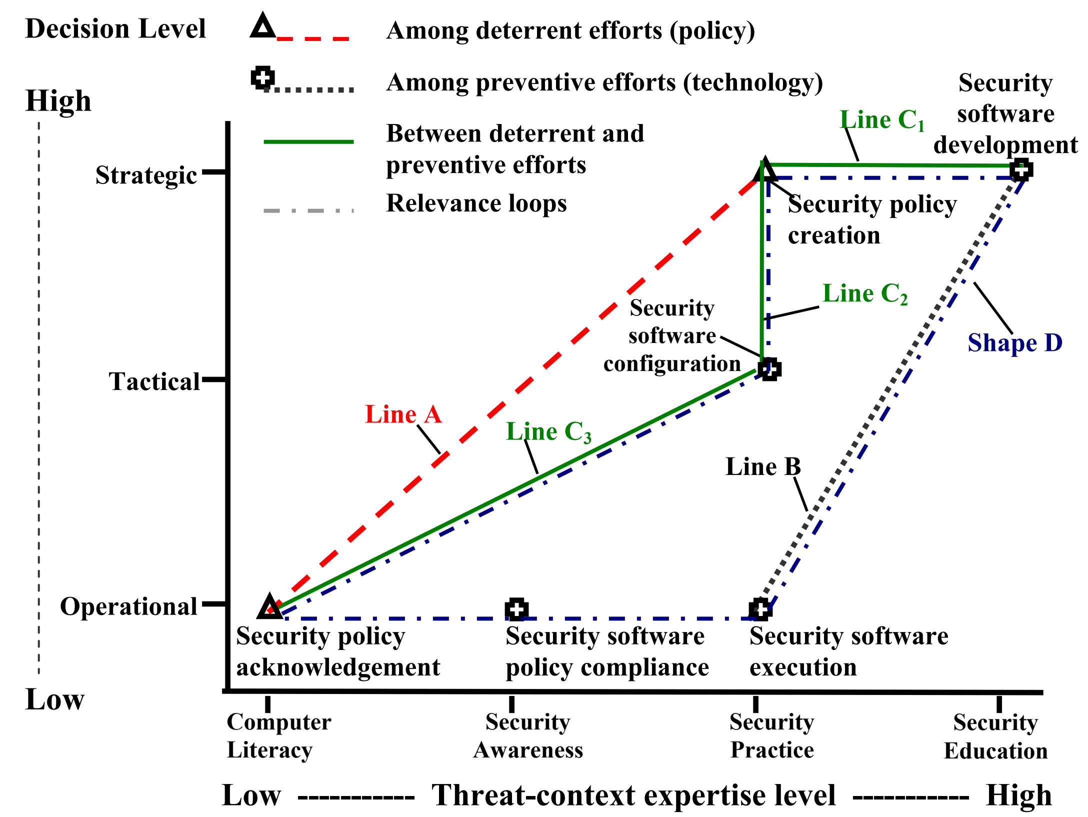

Decision Level
High
Low
Strategic
Tactical
Operational
Among deterrent efforts (policy)
Among preventive efforts (technology)
Between deterrent and preventive efforts
Relevance loops
Security software development
Line C_1
Security policy creation
Line C_2
Shape D
Security software configuration
Line A
Line C_3
Line B
Security policy acknowledgement
Security software policy compliance
Security software execution
Computer Literacy
Security Awareness
Security Practice
Security Education
Low ---------- Threat-context expertise level ---------- High

Figure 6

Schou and Trimmer (2004) also suggested that modern IS complexity requires a defense in depth based on security awareness (e.g. threat-context expertise), policy (e.g. deterrent security efforts), and technology (e.g. preventive security efforts). Deterrent and/or preventive efforts represent operational, tactical, and strategic security decisions. Deterrent and/or preventive security efforts require threat-context expertise for functionality. The level of expertise should follow the Schou and Trimmer learning hierarchy. The level of expertise should also vary over the specific type (strategic, tactical, or operational) of security decision that represents the deterrent and/or preventive effort. Figure 6 illustrates the threat-context expertise needed for security decisions. Deterrent efforts and/or preventive efforts can span wide user-level continuums between security decision type and threat-context expertise.

For a deterrent example, line A on Figure 6 represents two points. The first point is a strategic decision to create security policy, which requires expertise in security practice. The second point is an operational user decision to acknowledge the security policy, which requires computer literacy. For a preventive example, line B on Figure 6 also represents two points. The first point is security software development, which requires strategic decisions and expertise from threat-context education. The second point is an operational decision to run the security software, which requires expertise in security practice.

Even wider continuums of threat-context expertise and security decisions exist when preventive efforts and deterrent efforts combine. Lines C_1, C_2, and C_3 on Figure 6 represent four stages that exist when security software is developed, adopted into security policy, implemented, and acknowledged. The first stage occurs during security software development, when strategic decisions require threat-context expertise from security education. The second stage occurs when strategic decisions, which require expertise in security practice, result in the adoption of the security software into policy. Line C_1 represents the shift in threat-context expertise between security education and practice. The third stage occurs during tactical decision-making. During the implementation and configuration of security software, tactical decisions require expertise in security practice to ensure proper functionality (Hawkins et al., 2000). Line C_2 represents the shift in decision-making between strategic and tactical security decisions. At the operational level, stage four occurs when user compliance to the new security software policy requires computer literacy. Line C_3 represents the shift in threat-context expertise between security practice and computer literacy.

The introduction of best practices (Bartoli, Hermel, and Ramis-Pujol, 2003) results in potential learning cycles from preventive (technology) and deterrent (policy) security effort combinations. Shape D reflects the potential relevance loops or learning cycles from situations as lines C_1, C_2, and C_3. Therefore, preventive and deterrent security efforts should provide threat-context knowledge transfer among users.

Information Security Awareness Construct

Effective information security starts with the basics (Egan, 2004). Therefore, perspectives and items that represent information security awareness should meet basic operational or user-level information security concerns. Whitman and Mattord (2004) noted that smaller organizations commonly outsource many higher-level IT functions. Organizational size should not differentiate among the information security concerns for desktop computer management, computer virus protection, and local-area-network issues. These types of information security concerns are applicable to basic user-level information security awareness in both business and home computing-environments. Therefore, in developing an information security awareness construct, we should consider two questions:

RQ1. What is the domain of information security awareness?

RQ2. What are measures of information security awareness?

"A domain definition of a concept is the specific meaning of interest for a given research context and an adequate domain can be extremely useful in furthering a topic of interest to academic societies" (Templeton, 2000, p. 57). A goal of this dissertation is to influence further research on the awareness and the practice of information security by providing a consensus definition that agrees with all or most previous research to date. The literature expresses three interrelated perspectives of technology, policy, and threat-context for a definitional meaning of information security awareness (ISA). The primary analysis level is the individual IS user. However, an additional demographic perspective provides individual and organizational levels for ISA analysis.

Attributes of ISA Defined

View	ISA Attribute	Generic Description
Demographic	Individual	Descriptive data about individual users
	Organizational	Descriptive data about organizational users
Technology	Individual	Descriptive data about home computing capabilities and user computer literacy
	Organizational	Descriptive data about business computing capabilities and user computer literacy
	Application	Understanding technology application to meet information security concerns
Policy	Formal	User behavior concerning information security that is required or recommended by the owner
	Informal	User behavior concerning information security that is recommended by other users
Threat-context	Physical Security	Understanding threats to ownership
	User Authentication	Proving trusted identity
	Access Control	Discerning authorized rights and privileges
	Encryption	Understanding why and when to make data unreadable to unauthorized use
	Security Management	Understanding the consequences of operational security decisions and maintenance activities

Table 7

Tables 7, 8a, 8b, and 8c illustrate evidence of literature support for these perspectives and define the components of these views. Table 7 provides short attribute descriptions for components of each ISA view. Tables 8a and 8b show respective individual and organizational ISA demographic and technology variables and variable responses, with expected direction of relationships. Table 8c shows the item response variables and direction of ISA relationships for ISA measurement of technology, policy, and threat-context views. The following sections explain each of the four ISA perspectives.

Demographic perspective. The literature provides a theoretical basis for the belief that certain traits describing groups or individuals should influence differences in ISA measurement. The demographic perspective views an individual trait as influencing ISA. The demographic perspective views a group trait as indirectly reflecting ISA with varied effectiveness. Individual and organizational demographic variables segment these traits (see Table 8a). The demographic variables also provide unit-analysis interest among the other technology, policy, and threat-context views.

Individual demographic variables should reflect different levels of ISA measurement. Age, gender, and education level can affect an individual's learning style. Different ways of learning suggests that subscale ISA means for each variable can vary among age, gender, and education level groups. Years of computer use can directly affect computer literacy. Increased computer literacy, through increased computer use, should positively affect the technology view of ISA.

Organizational demographics should also reflect different levels of ISA. College classification and college major are for use only in pilot testing. However, MIS majors have potentially higher computer literacy and familiarity with the information security concept by the nature of their studies. Job classification and area of work can also suggest computer literacy and information security familiarity because of individual job descriptions and similar knowledge required for work responsibilities. The A/P (academic and professional) job classification should have higher computer literacy and information security familiarity due to the concentration of IT specialist jobs. Thus, ISA subscale means among organizational demographic variables should differ among job classification and area of work groups.

Nature of Demographic Variables Expected to Influence ISA

Level	Variables with potential responses (expected relationship direction)
Individual	Age: < 19, 19-24, 25-29, 30-34, 35-39, 40-44, 45-49, 50-54, 55-59, 60-64, > 64
	Gender: Female, Male
	Education Level: some H. S., H. S. diploma, technical school, some college, college diploma, some graduate school, 1st graduate degree, 2nd gradate degree
	Years of computer use: < 1, 01-03, 04-06, 07-10, 11-13, 14-16, 17-20, 21-25, 25-30, > 30 (+)
Organizational (Student*)	College Classification: freshman, sophomore, junior, senior, graduate school
	College Major: Accounting, Aviation Mgt., Logistics, Economics, Finance, Mgt., MIS**, Mktg., Other
Organizational (Non-student)	Area of work: Administration, AAES, ACES, Agriculture, Architecture, Business, Education, Engineering, Forestry, Graduate, Honors, Human Sciences, Liberal Arts, Nursing, Outreach, Pharmacy, COSAM, Veterinary Medicine
	Job Classification: staff, A/P**, NTF, Faculty

* For college student responses in pilot testing.
** Expected superior trait within discontinuous variables

Table 8a

Technology perspective. Schou and Trimmer (2004) stated that technology is the most obvious and expensive countermeasure, which summarizes the technology view. The technology perspective views ISA as an assortment of hardware and software capabilities that individual IS users, with sufficient computer literacy, manipulate as tools

(Hawkins, Yen, and Chou, 2000). However, the costs associated with technology acquisition, implementation, and training can be prohibitive (Sandhu, 2003). The information security literature provides a theoretical basis leading to the belief that different technology capabilities and associated computer literacy will affect ISA.

Nature of Technology Variables Expected to Influence ISA

Level	Variables with potential responses (expected relationship direction)
Individual	Home hrs. of average weekly computer use: < 1, 01-05, 06-10, 11-15, 16-20, 21-25, 16-20, 21-25, 26-30, 31-35, 36-40, > 40 (+)
	Home computer operating system (OS): none; DOS; Linux; MAC; Windows 3.x, 95, 98, NT, 2000, ME, XP; Do not know
	Home local-area-network (LAN) connection: none, hub router, wireless router combo, do not know
	Home Internet connection: none, dial-up, DSL, cable, satellite, do not know
	Home hrs. of average weekly Internet use: < 1, 01-05, 06-10, 11-15, 16-20, 21-25, 16-20, 21-25, 26-30, 31-35, 36-40, > 40 (+)
Organizational	Business hrs. of average weekly computer use: < 1, 01-05, 06-10, 11-15, 16-20, 21-25, 16-20, 21-25, 26-30, 31-35, 36-40, > 40 (+)
	Business computer OS: none; DOS; Linux; MAC; Windows 3.x, 95, 98, NT, 2000, ME, XP; do not know
	Business LAN connection: none, hub router, wireless router combo, do not know
	Business Internet connection: none, dial-up, wired, wireless, do not know
	Business hrs. of average weekly Internet use: < 1, 01-05, 06-10, 11-15, 16-20, 21-25, 16-20, 21-25, 26-30, 31-35, 36-40, > 40 (+)

Table 8b

Identifying technology capabilities and associated computer literacy should provide one ISA measure of this view. Table 8b lists technology variables that distinguish certain technology capabilities and computer literacy indicators. Table 8b also differentiates between individual and organizational technology because technology can differ between computing-environments (e.g. home versus business, business versus business, or home versus home).

Individual and organizational technology variables should affect ISA measurement. Hours of average, weekly computer use and/or Internet use can directly influence computer literacy. Increased computer literacy, from increased computer use and/or Internet use, should positively affect ISA measurement.

Individual and organizational technology variables should also affect different levels of ISA measurement. Computer operating systems are varied and complex. Adding local-area-network and/or Internet connectivity will increase operating system capabilities and operating system complexity. Increases in technology capabilities and complexity necessitate increases in associated computer literacy for functionality. Thus, ISA subscale means among individual and organizational technology variables of computer operating system, local-area-network connection, and Internet connection should differ among each variable's groups.

Through the technology view, ISA represents an individual IS user applying a specific, appropriate technology for a specific security concern. Hawkins et al. (2000) illustrated the technology view with the variety of technologies made available to secure Internet computing. A second ISA measure from the technology view is user comprehension, or understanding specific technologies to address specific security concerns. Schou and Trimmer (2004) stated, "…information technology security is a core business process. Integral to establishing a core process is building a competent information technology security work force—a people based countermeasure" (p. ii). As an example, a competent computer user knows and understands why virus protection software requires frequent updates to be effective.

Table 8c lists technology (T) item-response variables that should influence ISA measurement. These variables should distinguish user comprehension about technology use for specific security concerns. Consistent application of appropriate technology to address a specific security concern should form a learned information security practice. This type of information security practice reflects an IS user's individual technology view of ISA.

Policy perspective. An issue-specific security policy adheres to particular rules of acceptable security behavior within a specific IS activity, such as email or Internet usage (Whitman and Mattord, 2004). Similarly, the policy perspective views ISA as a set of acceptable user behaviors that follow a certain security pattern. Users act out the behavioral security pattern during issue-specific IS activities to represent ISA. The information security literature provides a theoretical basis leading to the belief that strong security policy acted out by individual users will affect ISA.

Schlarman (2002) viewed policies and standards as forming the backbone of a security program. Thomson and von Solms (2005) showed how formal policy follows management directives and suggestions, while informal policy follows other IS user suggestions or advice. The policy view represents ISA through either recommended or required user behavior in response to security concerns. A user having virus protection software running on his or her desktop computer because of a company virus-protection policy is a formal policy example. A user choosing not to open a strange email attachment from an unknown sender because of another user's advice is an informal policy example. From the policy view, an ISA measure would require wording an item variable (question) in the context of a specific, desired security behavior that distinguishes the user's compliance to a given security policy. Table 8c lists policy item-response variables from formal (FP) and informal (IP) security policies.

Repetition of issue-specific security behavior can lead to regularity, structure, and ultimately knowledge transfer (Bartoli, Hermel, and Ramis-Pujol, 2003). The result is a learned information security practice. From the policy view, an information security practice reflects individual user-level ISA, learned over time through repetition of recommended or required security policy.

Threat-context perspective. The threat-context perspective views ISA as user knowledge. Knowledge of where potential IS security threats exist and an understanding of the appropriate countermeasures. The information security literature provides a theoretical basis for the belief that user-level, threat-context knowledge will affect ISA. Table 8c lists threat-context item-response variables (C), which reflect the composite threat-context view that an individual user's threat-context knowledge plays a significant role in maintaining information security.

The literature also shows an apparent lack of effective individual user training for threat-context knowledge in organizations. Most of the literature calls for additional training programs, but leaves the questions of why, where, what, who, and how unanswered. Siponen (2001) proposed selective interest groups among the following five dimensions of information security awareness: organizational, general-public, socio-political, computer-ethical, and institutional-education. Each dimension and associated interest group answers the respective why and where questions. Furnell et al. (2002)

suggested a technology answer that offers prototype, computer-based training to simulate “what if” threat-context scenarios. If the concept matures, this technology suggests how the training could commence. The “with whom” and “to what extent” training questions remain. User-level ISA measurement, through a detailed threat-context view, could provide answers to both remaining questions by identifying individuals who lack specific threat-context scenario knowledge.

A challenge exits in condensing security threats and associated countermeasures into item-response variables that capture the numerous threat-context scenarios. However, both Weber (1988) and Ferrarini (2001) noted the security problems associated with information access-points. Information access-points exist within IS as read, write, and/or execute capabilities. Authorized users (e.g. people, software, computers, or other IS) obtain legal read, write, and/or execute capabilities (Whitman and Mattord, 2005). All other capabilities are illegal and potentially insecure. Ferrarini (2001) suggested focusing security priority among five information access points: physical security, user authentication, access control, encryption, and security management. Table 7 provides a short attribute description for each information access point. Accessing user-level item-response variables among these information access points could provide a detailed threat-context view to ISA measurement. For this perspective, item-response variable measures would require content knowledge concerning a given information access point vulnerability. The technology and policy views may also reflect information access point scenarios. However, these two views focus the application of technology or policy to provide ISA behavior. The following discussions explain the rationale for advancing these five information access points as threat-context classes for item-response variables listed in Table 8c.

Physical security requires understanding how to minimize threats that compromise physical ownership (Schneier, 2002). Natural disasters, theft, or IS component failure are examples of physical security threats (Weber, 1988). However, a current, restorable backup of IS data is a vital first step in physical computer security (Kearvell-White, 1996; Aytes and Connolly, 2004). An item measure for user-level understanding in the necessity of a current, restorable data backup should reflect a physical security threat-context (TP) measure of ISA (see Table 8c).

User authentication requires establishing proof of trusted identity (Menascé, 2003; Whitman and Mattord, 2005). The traditional and ubiquitous approach to authentication is the knowledge of a unique password (Schneier, 2002; Marks, 2005). However, a password is effective only if an individual user is the only user that knows it (Smith, 1987; Zviran and Haga, 1999; Marks, 2005). An item measure variable of user-level understanding in the necessity of password confidentiality should reflect a user authentication, threat-context (TU) measure of ISA (see Table 8c).

Access Control requires discerning the rights and privileges of users, software, and other computers to use, manipulate, modify or affect IS components (Fink, 1995; Schneier, 2002; Whitman and Mattord, 2005). IS components may be the subject or object of access control, depending on the situation. A subject may have the right to access an object, or an object may extend the privilege to allow a subject access (Schneier, 2002). Legitimate rights and privileges are legal access and all other access is illegal (Whitman and Mattord, 2005). Limiting the access of IS resources only to authorized persons, programs, processes, or other IS is a complex task (Fink, 1995). Unfortunately, users cannot physically view who or what (subjects) access hardware, software, and data resources (objects) inside a computer. However, user understanding of the illegal access impact to IS components and the associated software used to restrict or detect the associated illegal access reflects crucial security skills (Sanders, 2003).

Practitioners and industry surveys note that common illegal access to desktop computers result from network intrusion or attacks and browser or email vulnerability to viruses, spyware, adware, or spam (Larsen, 1999; Mendelson, 2000; Stahl, 2001; D'Antoni, 2002; Hulme, 2002; Sarrel, Ellison, and Kaven, 2003; Hulme, 2004; Lipschutz, 2004; Franklin, 2005: Hulme, 2005). Newer operating systems can restrict network intrusion to shared devices. Network firewalls can block external attacks against logical TCP/IP ports. Personal firewall software can identify and block access to and from logical TCP/IP ports of desktop computers. Virus protection software can identify and remove or block malicious code in the form of viruses, spyware, or adware. Email filters can remove or block unsolicited email or spam. User-level understanding of these access control threats and countermeasures should reflect an access control, threat-context (TA) measure of ISA (see Table 8c).

Encryption is a basic security component in Internet computing applications ranging from email to e-commerce transactions (Menascé, 2003). Encryption requires user-level understanding of why and when to make certain data unreadable to unauthorized use. Understanding why data requires encryption should determine when the security protocols and associated encryption methods are necessary. Common data and data file examples of sensitive information are credit-card numbers, social-security numbers, confidential emails, or confidential documents. User-level understanding that these types of information require protection from unauthorized use should reflect an encryption, threat-context (TE) measure of ISA (see Table 8c).

Technology, Policy, and Threat-context Variables Expected to Measure ISA

ISA View	With respect to information technology and its security, I am aware… Item-response Variable	(expected relationship direction)
T, TA	A01 Virus protection software can identify and remove known viruses	(+)
T, TS	A02 Virus protection software requires frequent updates	(+)
T, TA	A03 Firewall software can block network attacks	(+)
T, TA	A04 Personal firewall software can block logical port access to/from a computer	(+)
FP, TU	A05 Acceptable Use Policy strongly suggests keeping passwords safeguarded	(+)
FP, TS	A06 Virus Protection Policy requires use of available software and updates	(+)
FP, TE	A07 OIT offers virtual private network (VPN) software for outside of intranet use	(+)
FP, TS	A08 Virus Protection Policy requires restricted access for computers with viruses	(+)
FP, TU	A09 Acceptable Use Policy dictates that wired and wireless network access requires a user-id and password	(+)
IP, TA	A10 other users suggest that computer viruses can infect emails or attachments	(+)
C	A11 as a user, my knowledge of computer threats plays a significant role	(+)
C, TP	A12 a current, restorable data back-up is necessary	(+)
C, TU	A13 password secrecy is fundamental	(+)
C, TA	A14 of the impact that a virus can have on a computer system	(+)
C, TA	A15 of the impact that spyware or adware can have on a computer system	(+)
C, TA	A16 of the impact network attacks can have on a computer system	(+)
C, TA	A17 of vulnerability with shared devices such as files, drives, or printers	(+)
C, TE	A18 encryption can deter unauthorized access to sensitive information (i.e. credit card numbers, social security numbers, confidential emails or documents)	(+)
C, TS	A19 Software requires periodic decisions and updates	(+)

ISA View Key:

Technology (T)	Threat-context (C)	C: User Authentication (TU)
Formal Policy (FP)	C: Physical (TP)	C: Access Control (TA)
Informal Policy (IP)	C: Encryption (TE)	C: Security Management (TS)

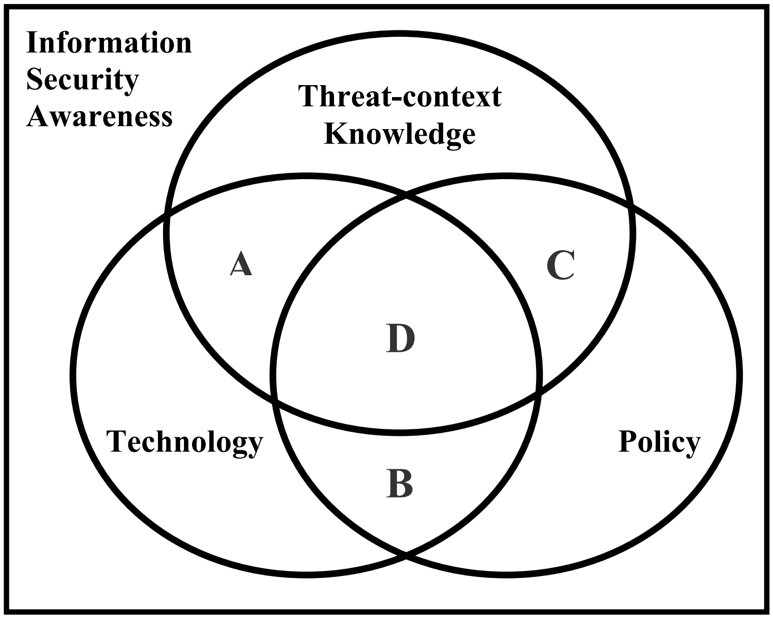
Table 8c

Security management requires understanding the consequences of operational security decisions. Operational security decisions affect the management of software updates/patches and the maintenance of software updates/patches. All software requires periodic updates and version patches for improved functionality. However, many of the updates and patches are for security concerns. Microsoft Corporation stated that managing software updates is vital to maintaining client computer security (Microsoft, 2004a). User-level understanding of software updates and patches should reflect a security management, threat-context (TS) measure of ISA (see Table 8c).

Rationale for combining perspectives. Schou and Trimmer (2004) noted ISA interrelationships among policy, technology, and threat-context knowledge perspectives. Policy dictates ISA behavior. However, users may not comply with the policy. Technology provides ISA capability. However, users may not have sufficient computer literacy to recognize and/or use the technology capability. Threat-context knowledge produces ISA. However, users may not have specific threat-context knowledge for all ISA scenarios. Figure 7 illustrates the rational for combining these perspectives.

Relationship A represents threat-context knowledge learned from computer literacy and technology capability or the computer literacy and technology capability gained from threat-context knowledge. Technology or security software (e.g. authentication, virus protection, firewalls, or virtual private network) requires threat-context knowledge for functionality. Software development requires technology capability. Software implementation requires computer literacy. Therefore, computer illiterate users can gain computer literacy and technology capability by learning specific security software. Computer literate users can learn threat-context knowledge from technology capability by using specific security software. Furthermore, threat-context knowledge can develop technology capabilities from computer literacy.

Technology, Policy, and Threat-context Perspectives of ISA



Expected relationships among ISA perspectives

A – Threat-context knowledge learned from computer literacy and technology capability, or
Computer literacy and technology capability gained from threat-context knowledge.

B – Computer literacy and technology capability gained from security policy compliance, or
Security behavior learned from computer literacy and technology capability.

C – Threat-context knowledge gained from security behavior, or
Security behavior learned from threat-context knowledge.

D – Threat-context knowledge gained from policy and technology, or
Security behavior learned from technology and threat-context knowledge, or
Computer literacy and technology capability gained from policy and threat-context knowledge.

Figure 7

Relationship B represents computer literacy and technology capability gained from acting out security behavior or security behavior learned from computer literacy and technology capability. Policy dictates behavior. Security policy can dictate specific security software use. Software use requires computer literacy. Software use provides a specific technology capability. Therefore, computer illiterate users can learn computer literacy and technology capability from security policy compliance. Furthermore, computer literate users can learn security behavior from security software use for a specific technology capability.

Relationship C represents security behavior learned from threat-context knowledge or threat-context knowledge gained from security behavior. Policy dictates behavior. Security policy development requires threat-context knowledge. Security policy compliance requires users acting out a specific security behavior. Therefore, users that act out a specific security policy behavior can learn specific threat-context knowledge. Furthermore, specific threat-context knowledge can develop user security behavior.

Relationship D combines policy, technology, and threat-context knowledge ISA relationships. The information security literature supports these ISA relationships. Threat-context knowledge gains are available from policy and technology (Furnell et al., 2002; Schou and Trimmer, 2004; Ma and Pearson, 2005). Learned security behavior is available through technology use and threat-context knowledge (Thomson and von Solms, 1988; Schou and Trimmer, 2004; Stanton, Stam, Mastrangelo, and Jolton, 2005). Computer literacy and technology capability are available from policy and threat-context knowledge (Hawkins et al., 2000; Aytes and Connolly, 2004; Schou and Trimmer, 2004). Relationship D represents ISA from the combined policy, technology, and threat-context knowledge perspectives. Therefore, users that act out specific security policy, users that deploy specific security software, and users that possess specific threat-context knowledge all represent user-level ISA.

Information Security Practices or Trends

Ma and Pearson (2005) investigated “best practices” by information security professionals and noted that guidelines, frameworks, or checklists are only part of the whole information security process. Hawkins, Yen, and Chou (2000) examined Internet security as a collection of technologies to protect IS utility and suggested that such technology requires computer literacy and ISA training among users. Whitman and Mattord (2004) included a viewpoint from Stephen Kahan, President of the Human Firewall Council, which summarized the current interests in improving and standardizing information security practice. Kahan said that information security savvy users form a layer of protection from within the organization to its security perimeters. A protection layer, whose information security practice, deters and prevents threats to an organization’s critical information assets. Schou and Trimmer (2004) labeled this protection layer a people based countermeasure. Improvement and standardization in user-level information security practice or behavior also appears in the literature (Straub, 1990; Straub and Nance, 1990; Fitzgerald, 1995; Harrington, 1996; Straub and Welke, 1998; Huston, 2001; Walters, 2001; Wu and Rocheleau, 2001; Piessens, Decker, and Win, 2002; Menascé, 2003; Sandhu, 2003; Leach, 2003; Aytes and Connolly, 2004; Stahl, 2004; Ma and Pearson, 2005; Stanton, Stam, Mastrangelo, and Jolton, 2005).

Studies have empirically tested information security practice within a computing-environment (Aytes and Connolly, 2004; Stanton, Stam, Mastrangelo, and Jolton, 2005). Stanton et al. (2005) examined survey results for password management and use. The authors used behavioral intentions, over a continuum between malicious to benevolent, to show that expertise was required within each behavioral intention level to determine the impact of the particular intention to harm or help IS utility. Figure 8 depicts the relationships that the authors proposed between behavioral intentions and expertise. They also cited the usefulness of self-reported practices (practice self-efficacy) for neutral and positive intentions where users were more likely to reveal these behaviors.

Two-factor taxonomy of end-user security behaviors.
(Stanton, Stam, Mastrangelo, and Jolton, 2005)

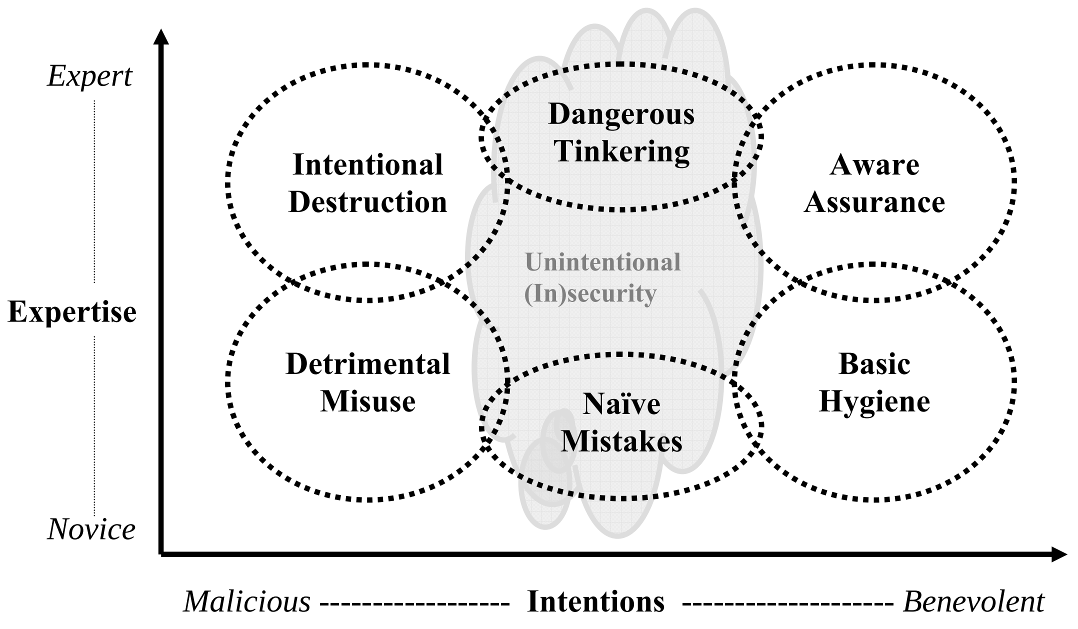


Figure 8

Aytes and Connolly (2004) investigated potential risky behaviors associated with password usage, email usage, and data backup. The authors based the study on the theory of reasoned action (Fishbein and Ajzen, 1975). The study placed safe computing behavior in the context of a user's intention to employ safe computing behaviors, or rational choice about a particular safe behavior and the consequences of not engaging in that particular safe behavior. Based on the user's perception, the study found evidence to support a connection between self-claimed expertise in safe computing (awareness self-efficacy) and self-reported user practices (practice self-efficacy).

Aytes and Connolly (2004) also called for the development of a research model that concentrates on factors most directly related to user's acceptance of countermeasures and incorporates user's perceptions and decision-making processes to improve information security. Such a research model could employ the ISA perspectives of policy, technology, and threat-context to investigate user-level security practices within computing-environments. However, policy and technology can differ among computing-environments, which could affect ISA measures. Further discussions on computing-environments follow.

Computing-environments

The National Computing Centre (1998; 2000) conducts business information-security surveys. Both the 1998 and 2000 surveys indicated that employees in small to medium-sized organizations' have less ISA than large organizations. Kankanhalli et al. (2003) found similar results and suggested that larger organizations have greater resources to expend on deterrent security efforts (i.e. policy). Smaller organizations, fewer than 100 individuals, have less structure and more centralization in their operations, with minimal formal security policies or measures and multiple roles delegated to individuals (Whitman and Mattord, 2004).

Increasingly, individuals take their work out of protected office (business computing) environments and into home computing-environments, which have more risk (Trouble with homework, 1994). Home computing-environments can support access to Internet computing (Lyytinen and Rose, 2003) that requires Internet security (Hawkins et al., 2000). However, technology between business computing-environments and home computing-environments can differ.

Tunyaplin, Lunce, and Maniam (1998) noted that telecommuting from a home computing-environment as opposed to physically commuting to the business computing-environment was an employee preference two to three days per week. Wattell (2002) noted that over 38 million workers in the United States reside in home computing-environments (as reported by IDC, a subsidiary of International Data Group). However, home computing-environments may lack policy and technology perspectives of ISA.

Information Security Practice Constructs

Leach (2003) suggested that a well-focused information security program targeted at improving user security behavior and decision-making skills could reduce security-related overhead. User-level deterrent and preventive security practices, associated with desktop computer management, virus protection, and local-area-network security issues, should reflect user-level ISA from threat-context, policy, or technology views in both business and home computing-environments. Two research questions develop for defining an information security practice construct using these basic security concerns and ISA perspectives:

RQ3. Which information security practices reflect ISA?

RQ4. Do security practices differ between computing-environments?

A research model, that includes ISA measurements and ISA measurements reflected in information security practices between business and home computing-environments, should represent the amount of ISA practiced in each computing-environment. User-reported measurements from each ISA perspective should reflect user-reported measurements for corresponding practice in each computing-environment. User-reported measurements for information security practice at work could affect user-reported measurements for information security practice at home, due to differences in policy and technology between the computing-environments. User-reported measurements for corresponding practices between work and home could distinguish information security obedience from ISA. Figure 9 illustrates an ISA model where information security practices reflect user-level ISA between business and home computing-environments.

User-level ISA between Environments

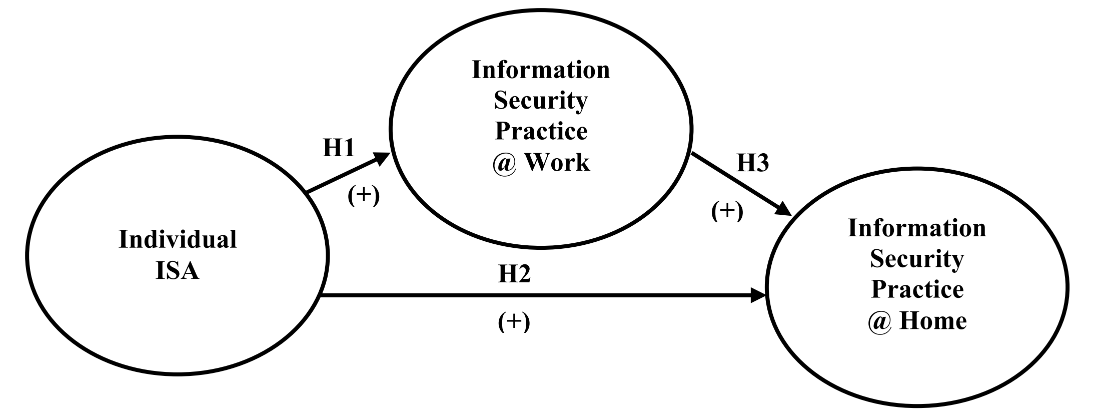

Information Security Practice @ Work
H1
(+)
H3
(+)
Individual ISA
H2
(+)
Information Security Practice @ Home

Figure 9

Tables 9 and 10 show the item-response variables and the expected direction of relationships for ISA measurement of technology, policy, and threat-context views of information security practice. Table 9 lists the item-response variables for security practice at work. Table 10 lists the item-response variables for security practice at home. Explanations for each of the hypothesized relations H1, H2, and H3 follow.

Relationship H1 represents the affect that combined ISA perspectives of policy, technology, and threat-context have on information security practice at work. Users who possess high levels of ISA should choose information security practice at work that reflects high levels of ISA.

> H1: Higher measures of user-level ISA should positively affect user information security practice at work.

Relationship H2 represents the affect that combined ISA perspectives of policy, technology, and threat-context have on information security practice at home. Users who possess high levels of ISA should choose information security practice at home that reflects high levels of ISA.

> H2: Higher measures of user-level ISA should positively affect user information security practice at home.

Relationship H3 represents the affect that information security practice at work has on information security practice at home. The literature supports the basis that computing-environments can differ. Home computing and business computing may differ with respect to policy and technology. Business-computing users who possess high levels of policy and technology perspectives of ISA could choose similar information security practice at home that reflects high levels of ISA.

> H3: Information security practice at work, which has high measures of user-level ISA perspectives of policy and technology, should positively affect user information security practice at home.

Information security practice must be business driven, user friendly, and "good enough", where the computing-environment is made secure as necessary, but not securer (Sandhu, 2003). Hence, computing-environments only require information security sufficiency because users may perceive information security practice as intrusive and/or a work impediment. User intentions toward IS was also a major determinant of a user's actual security behavior (Aytes and Connolly, 2004). Likewise, Lewis, Agarwal, and Sambamurthy (2003) noted that individual beliefs about technology have subsequent impact on individual behaviors toward IS use. Therefore, the need exists to discuss individual human traits as they relate to IS use and ISA.

Information Security Practice at Work Variables Expected to Measure ISA

ISA **View**	**On business computer systems…** **Item-response Variable**	(**d**eterrent and/or **p**reventive) (expected relationship)
FP, TU	W01 I log off when I leave a computer system	(**p**) (+)
FP, TA	W02 I shut down and power off when leaving a computer system	(**p**) (+)
FP, TU	W03 All of my computer sessions require a unique user-id and password	(**p**) (+)
IP, TP	W04 I backup my data on reliable media (disks, CDRW, etc)	(**p**) (+)
IP, TP	W05 I test the restorability of back-up files that I have created	(**p**) (+)
FP, TS	W06 I check that virus protection software is enabled and updated	(**p**) (+)
FP, TA	W07 I rely on university provided virus protection software and its updates	(**p**) (+)
TS, T	W08 I check for new versions of virus protection software	(**p**) (+)
TS, T	W09 I review virus protection software logs for updates and drive scans	(**p**) (+)
TA, T	W10 Personal firewall software monitors traffic into/out of my computer(s)	(**p**) (+)
TA, IP	W11 As I surf the Web, I allow browsers to accept cookies from Web sites	(**p**) (-)
TA, T	W12 As I surf the Web, I allow browsers to download software as necessary	(**p**) (-)
TU, T	W13 I allow software to save user-ids and passwords for faster return visits	(**p**) (-)
TA, T	W14 I remotely connect to computers and share drives, printers, or files	(**p**) (-)
T, TA	W15 I use file transfer software to securely move files between computers	(**p**) (+)
T, TA	W16 I store email on my computer rather than the email server	(**p**) (-)
IP, TA	W17 I open emails regardless of knowing the originator's identity	(**d**) (-)
TE, T	W18 I encrypt confidential files with passwords	(**p**) (+)
TE, T	W19 I look for "https://" before I make Internet financial transactions	(**p**) (+)
TA, FP	W20 Other people share the computer(s) I routinely use for Internet access	(**d**) (-)
TA, T	W21 Viruses affect the performance of my computer	(**p**) (+)
T, TA	W22 Virus protection software identifies/limits virus impact to my computer	(**p**) (+)
TU, FP	W23 I routinely choose to change my password(s)	(**d**) (+)
TP, FP	W24 I use a character sequence like Ij4Gf4Se%f# as my computer password	(**d**) (+)

Technology (T)	Threat-context (C)	C: User Authentication (TU)
Formal Policy (FP)	C: Physical (TP)	C: Access Control (TA)
Informal Policy (IP)	C: Encryption (TE)	C: Security Management (TS)

Table 9

Information Security Practice at Home Variables Expected to Measure ISA

ISA View	On home computer systems… Item-response Variable	(**d**eterrent and/or **p**reventive) (expected relationship)
TU	H01 I log off when I leave a computer system	(**p**) (+)
TA	H02 I shut down and power off when leaving a computer system	(**p**) (+)
IP, TA	H03 All of my computer sessions require a unique user-id and password	(**p**) (+)
TP	H04 I backup my data on reliable media (disks, CDRW, etc)	(**p**) (+)
TP	H05 I test the restorability of back-up files that I have created	(**p**) (+)
IP, TS	H06 I check that virus protection software is enabled and updated	(**d**) (+)
FP, TA	H07 I rely on university provided virus protection software and its updates	(**d**) (+)
TS, T	H08 I check for new versions of virus protection software	(**p**) (+)
IP, TS	H09 I review virus protection software logs for updates and drive scans	(**d**) (+)
TA, T	H10 Personal firewall software monitors traffic into/out of my computer(s)	(**p**) (+)
TA, T	H11 As I surf the Web, I allow browsers to accept cookies from Web sites	(**p**) (-)
TA, T	H12 As I surf the Web, I allow browsers to download software as necessary	(**p**) (-)
TA, T	H13 I remotely connect to computers and share drives, printers, or files	(**p**) (-)
T, TA	H14 I use file transfer software to securely move files between computers	(**p**) (+)
T, TA	H15 I store email on my computer rather than the email server	(**p**) (-)
IP, TA	H16 I open emails regardless of knowing the originator's identity	(**p**) (-)
TE	H17 I encrypt confidential files with passwords	(**d**) (+)
TE, T	H18 I look for "https://" before I make Internet financial transactions	(**p**) (+)
TA, IP	H19 Other people share the computer(s) I routinely use for Internet access	(**d**) (-)
TA, T	H20 Viruses have affected the performance of my computer	(**p**) (+)
T, TA	H21 Virus protection software identifies/limits virus impact to my computer	(**p**) (+)
TU, IP	H22 I routinely choose to change my password(s)	(**d**) (+)
TP, T	H23 I use a surge protector and/or an uninterruptible power supply (UPS)	(**p**) (+)
TA, T	H24 All wired or wireless access to the Internet is password protected	(**p**) (+)
TU, IP	H25 I use a character sequence like Ij4Gf4Se%f# as my computer password	(**d**) (+)
T, TA	H26 I allow unknown users to access files on my computer(s) through the Internet (i.e. music file sharing, personal Web Server, etc.).	(**p**) (-)
IP, TU	H27 I try to use the same password(s) for convenience	(**d**) (-)
T, TS	H28 I have other email account(s) forwarded to one main email account	(**p**) (-)
T, TS	H29 I use a spam filter on my email account(s)	(**p**) (+)
T, TA	H30 I have virus protection software on my computer	(**p**) (+)
T, TA	H31 I have shared devices (files, folders, drives, or printers) that are not password protected or user-id restricted.	(**p**) (-)
T, TA	H32 Computer systems or other appliances share my Internet connection	(**p**) (-)
T, TA	H33 I have personal firewall software on my computer	(**p**) (+)
IP, TU	H34 Other people know my password(s)	(**d**) (-)
TE, T	H35 I use VPN software to access other computers/computer networks	(**p**) (+)
TA, IP	H36 I turn off or disconnect the Internet connection(s) when not in use	(**p**) (+)
IP, TS	H37 I share information security concerns with other people that share my computer systems with Internet access	(**d**) (+)

Technology (T)	Threat-context (C)	C: User Authentication (TU)
Formal Policy (FP)	C: Physical (TP)	C: Access Control (TA)
Informal Policy (IP)	C: Encryption (TE)	C: Security Management (TS)

Table 10

Individual Human Traits and ISA

Lord, De Vader, and Alliger (1986) noted that human traits are important constructs for the perception of individual behavior. Individual human traits also impact user acceptance of technology (Hurt, Joseph, and Cook, 1977; Davis, 1989; Adams, Nelson, and Todd, 1992; Harrison and Rainer, 1992; Burton, 1994; Compeau and Higgins, 1995; McAdam, 2000; Chau, 1996; Man, 2001; Thatcher and Perrewè, 2002; Bartoli, Hermel, and Ramis-Pujol, 2003; Lyytinen and Rose, 2003; Sheng and Pearson, 2003) as well as adoption of technology (Kegerreis, Engel, and Blackwell, 1970; Raho, Belohlav, and Fiedler, 1987; Baptista, 1999; Fichman and Kemerer, 1999; Teng, Grover, and Güttler, 2002). More recently, Lewis, Agarwal, and Sambamurthy (2003) identified the individual factors of personal innovativeness and computer self-efficacy that influence individual beliefs about technology use within IS.

The Lewis et al. results also unexpectedly found that ease of use—from the theory of reasoned action (Fishbein and Ajzen, 1975) and the technology acceptance model (Davis, 1989; Adams, Nelson, and Todd, 1992; Chau, 1996)—did not seemingly influence individual beliefs about technology use. With respect to information security, the Lewis et al. results could explain technology ease of use versus consequences of information security risk. Information risk explains how financial and time costs, associated with deterrent and preventive efforts employed to minimize security threats, could be overshadowed by threat-context knowledge of the massive efforts (financial and time) required to restore IS after a full-scale security breach. A closer review of personal innovativeness and computer self-efficacy, the two factors identified by Lewis et al., could clarify the role of human traits in influencing ISA perspectives.

Personal Innovativeness

Hurt, Joseph, and Cook (1977) defined innovativeness as an underlying personality construct for an individual's willingness to change. Man (2001) also noted that innovation shifts paradigms and that the creation of new technologies can provide a foundation for innovation. Recall that IT innovations shifted the paradigm in information security. Information security practice subsequently had to shift in order to compensate and protect IS utility.

The Hurt, Joseph, and Cook (1977) personal innovativeness (PI) construct presented eight base item questions that were expandable to twenty. Responses to the PI items classified individuals among five categories: innovators, early adopters, early majority, late majority, and laggards. With respect to the ISA perspectives of policy and technology, responses to the PI items could also distinguish individuals among similar categories. Examples of these situations are the willingness to accept change in security behavior or use a recommended security software application over an individual preference. Each PI category would reflect stages of individual reluctance to gain technical expertise in deterrent and preventive security efforts needed to compensate for a corresponding paradigm shift in information security. Table 11 lists the twenty questions associated with the PI construct items as adapted to ISA.

Mann (2001) also discussed the link between creativity and innovativeness where innovativeness ventures past creativity into implementation. With respect to ISA, the categories of innovators, early adopters, and the early majority could become catalysts for organizational ISA and stronger individual ISA that encouraged compliance among the late majority and laggards. McAdam (2000) proposed a similar perspective to innovation where knowledge workers increased innovation by turning tacit knowledge into explicit knowledge along with passing tacit knowledge to others in the organization for use. Teng, Grover, and Güttler (2003) also supported this perspective in innovation diffusion where the distribution of technology (e.g. deterrent and preventive security efforts) would occur mostly through contacts among the organizational user culture and the diffusion process was essentially an imitation process. Until knowledge is transferred, both policy and technology perspectives of ISA depend on an imitation process of a given threat-context knowledge.

Personal Innovativeness (PI) Construct

(adapted from Hurt, Joseph, and Cook, 1977)

With respect to my approach toward information technology and its security…

PI01…my peers ask me for advice or information.
PI02…I enjoy trying out new ideas.
PI03…I seek out new ways to do things.
PI04…I am generally cautious about accepting new ideas. *
PI05…I frequently improvise methods for solving a problem when an answer is not obvious.
PI06…I am suspicious of new technology and new ways of thinking.
PI07…I rarely trust new ideas until I can see whether the vast majority of people around me accept them. *
PI08…I feel that I am an influential member of my peer group.
PI09…I consider myself to be creative and original in my thinking and behavior.
PI10…I am aware that I am usually one of the last people in my group to accept something new. *
PI11…I am an inventive kind of person.
PI12…I enjoy taking part in the leadership responsibilities of groups.
PI13…I am reluctant about adopting new ways of doing things until I see them working for people around me. *
PI14…I find it stimulating to be original in my thinking and behavior. *
PI15…I tend to feel that the old way of living and doing things is the best way. *
PI16…I am challenged by ambiguities and unsolved problems.
PI17…I must see other people using new technologies before I will consider them. *
PI18…I am receptive to new ideas and practices.
PI19…I am challenged by unanswered questions.
PI20…I often find myself skeptical of new ideas and practices. *

* Original eight questions

Table 11

From this discussion, one can propose that personal innovativeness has a positive relationship with ISA. Individuals who have a high PI measure should also have a high ISA measure.

H4: High measures of user-level PI should positively affect high measures of ISA.

Computer Self-efficacy

Bandura (1977, 1986) proposed self-efficacy as individual perception for having sufficient skills to perform given tasks, where the individual would also tend to do the tasks successfully. Bandura suggested that self-efficacy influenced choices concerning which behaviors to undertake that would ultimately lead to the mastery of the behaviors. Also, Nelson (1990) added that the successful use of IT depended on the technology itself and the skill level or expertise of the individual using the technology.

Compeau and Higgins (1995) defined computer self-efficacy (CSE) as judgment of an individual's own capability to use a computer in the accomplishment of some future task, which is individual perception of one's own computer skills. The authors developed a 10-item CSE scale, suggesting that CSE plays an important role in shaping individuals' feelings and behaviors about computer use when accomplishing tasks. With respect to the technology perspective of ISA, CSE could measure a computer user's perception of his or her ability (i.e. computer literacy) to perform security behavior such as use security software within a computing-environment. Table 12 denotes the questions (items scales) associated with the Compeau and Higgins (1995) CSE construct, as adapted for ISA.

Computer Self-efficacy (CSE) Construct

(Adapted from Compeau and Higgins, 1995)

In your opinion, could you install and set-up security software…

CSE01 …if there was no one around to tell me what to do as I go?

CSE02 …if I had never used another application like it before?

CSE03 …if I had only manuals for reference?

CSE04 …if I had seen someone else using it before trying it myself?

CSE05 …if I could call someone for help if I got stuck?

CSE06 …if someone else had helped me get started?

CSE07 …if I had a lot of time for the completion of the task(s)?

CSE08 …if I had just the built-in help facility for assistance?

CSE09 …if someone showed me how to do it first?

CSE10 …if I had used similar applications before to obtain the same goal?

Table 12

CSE is a dynamic individual trait because of the influence of others from intervention (Gist and Mitchell, 1992). Sheng and Pearson (2003) investigated the influence of organizational culture on CSE. Their results showed that teamwork demonstrated the strongest relationship with CSE among climate and morale, information flow, involvement, supervision, and meetings. Their results suggested that teamwork and information flow contribute most to an individual's CSE. With respect to ISA, individual team members would have various levels of computer literacy and threat-context knowledge with which to collectively engage in information security practice within a given computing-environment.

Thatcher and Perrewé (2002) investigated the relationships among dynamic, IT-specific individual differences (i.e. computer anxiety and CSE) and stable individual differences (i.e. PI, negative affectivity, and trait anxiety). They found that PI correlated positively with CSE and negatively with computer anxiety. The authors suggested that computer anxiety partially mediated PI's influence on CSE and neither trait anxiety nor negative affectivity influenced CSE. Harrison and Rainer (1992) also noted that individuals demonstrating higher computer skills also exhibited greater creativity (innovativeness). With respect to ISA, both PI and CSE can differentiate which users were more likely to engage in deterrent and preventive efforts within a computing-environment.

From this discussion, one can propose that computer self-efficacy has a positive relationship with ISA. Individuals who have a high CSE measure should also have a high ISA measure.

H5: High measures of user-level CSE should positively affect high measures of ISA.

Information Security Research Agenda

Disruptive IT innovations (Thomson and von Solms, 1988; Lyytinen and Rose, 2003) shift information security paradigms. These paradigm shifts affect the relationships (Thomson and von Solms, 2005) among information security, IT governance, and corporate culture.

Kankanhalli et al. (2003) identified ISA and organizational size as mitigating factors, which influence deterrent and preventive security efforts (information security practice) and impact information security effectiveness. Also, organizational size (Kankanhalli et al., 2003; Ma and Pearson, 2003; Whitman and Mattord, 2005) could affect the policy perspective of ISA among computing-environments. Similarly, computing-environments could also affect the technology perspective of ISA. Therefore, ISA could influence information security practices between computing-environments.

Lewis, Agarwal, and Sambamurthy (2003) suggested that individual factors of PI and CSE can influence individual beliefs about technology use within IS. Therefore, these two factors could also influence ISA.

The User-level ISA Concept

Aytes and Connolly (2004) called for the development of a research model that concentrates on factors most directly related to computer user's acceptance of countermeasures and incorporates user's perceptions and decision-making processes to improve information security. Combining the concepts of PI, CSE, individual ISA, and information security practices, Figure 10 depicts a research model to compare information security practice in formal, structured computing-environments (e.g. in a business environment) with security practice in informal, unstructured computing-environments (e.g. in a home computing-environment). The model in Figure 10 details the user-level ISA concept, which also supports the research call from Aytes and Connolly (2004).

The user-level ISA concept models individual ISA positively affecting both information security practices at work and at home. Differing computing-environments imply that the research requires user-level analysis among respondents who compute at work and at home. Beyond information security obedience, individual ISA learned through the user's information security practice in the business computing-environment would also positively affect the user's information security practice within the home computing-environment. Both CSE and PI would also positively affect an individual user's ISA and their subsequent security practice in both computing-environments.

Research Model for the User-level ISA Concept

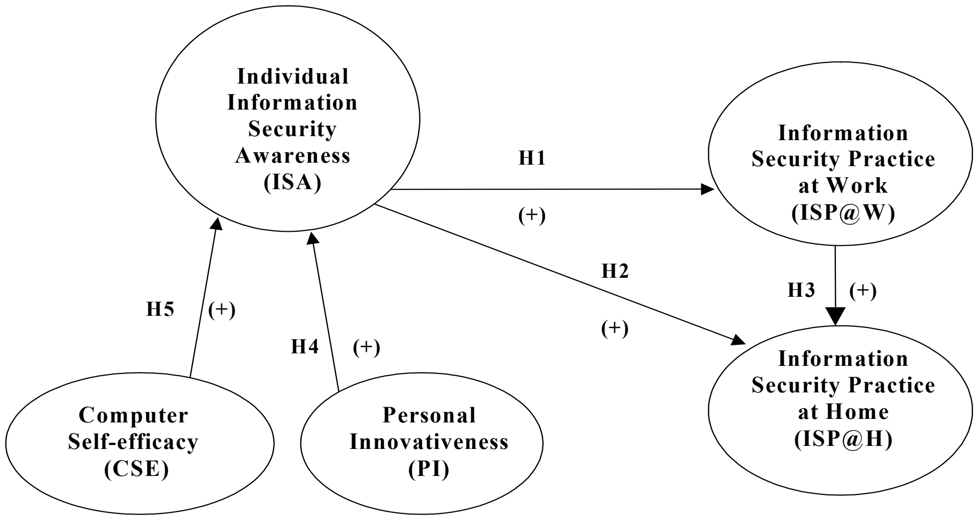

Individual Information Security Awareness (ISA)
Information Security Practice at Work (ISP@W)
Information Security Practice at Home (ISP@H)
Computer Self-efficacy (CSE)
Personal Innovativeness (PI)
H1
(+)
H2
(+)
H3
(+)
H4
(+)
H5
(+)

Figure 10

The research model, as the user-level ISA concept, depicts the previously noted hypothesis and addresses the following research questions:

RQ1. What is the domain of information security awareness?

RQ2. What are measures of information security awareness?

RQ3. Which information security practices reflect individual ISA?

RQ4. Do security practices differ between computing-environments?

RQ5. Does CSE influence individual ISA?

RQ6. Does PI influence individual ISA?

The next chapter discusses the methodology necessary to implement each phase of the research agenda for the user-level ISA concept.

CHAPTER III. METHODOLOGY

Introduction

This chapter describes the methodology used to address the research questions and hypotheses posed in Chapter II. Using traditional techniques, the research develops information security awareness (ISA) scale measures and information security practice measures that should reflect the awareness and practice of information security at work (ISP@W) and at home (ISP@H). Personal innovativeness (PI) and computer self-efficacy (CSE) use previously established scales. The study uses a comprehensive methodology derived from the works of Churchill (1979); Grover, Lee, and Durand (1993); Lewis (1993); Malhotra and Grover (1998); and Templeton (2000). Table 13 depicts the authors' contributions to the current methodology.

Research Design

This dissertation employs survey research in its design. Lewis (1993), and later Templeton (2000), successfully employed three methodological stages of survey research design in their dissertations. The three methodological stages are content analysis of the literature, instrument development, and computation of statistical profiles for ISA, ISP@W, ISP@H, PI, and CSE. These stages combine to provide an overall framework for the survey research methodology. Table 13 illustrates how the framework investigates the following research questions about the concepts being operationalized (ISA, ISP@W, ISP@H, PI, and CSE):

RQ1. What is the domain of information security awareness?
(Content analysis)

RQ2. What are measures of information security awareness?
(Instrument development)

RQ3. Which information security practices reflect individual ISA?
(Instrument development)

RQ4. Do security practices differ between computing-environments?
(Statistical profile)

RQ5. Does CSE influence individual ISA? (Statistical profile)

RQ6. Does PI influence individual ISA? (Statistical profile)

Churchill (1979) suggested traditional methods for developing marketing construct measures. The literature supports using these methods among different IS studies (Sethi and King, 1991; Lederer and Sethi, 1992; Grover, 1993; Rainer and Harrison, 1993; Sethi and King, 1994; Lewis, Snyder, and Rainer, 1995). Churchill proposed four instrument development phases that include 1) construct domain specification, 2) generation of items, 3) data collection, and 4) measure purification. These four phases focus on satisfying validity and reliability concerns, which require iterative development and testing.

Steps within each methodological stage identify particular research procedures that provide validity and reliability assessment. Content analysis from the literature review helps define the ISA domain and subsequent creation of ISA, ISA@W, and ISP@H scale

Research Methodology Framework

Stage, Research Question (Lewis, 1999)	**Phase** (Churchill, 1979)	**Step** (Lewis, 1993; Templeton, 2000)	**Procedure** (Templeton, 2000)	**SMA-n** (Grover, Lee, and Durrand, 1993)	**SA-n** (Malhotra & Grover, 1998)	**Deliverable**
Content Analysis: RQ1: What is the domain of ISA?	1	Define content domain	Literature review		1	Domain definition
			Operationally define			Operational definition
		Criteria creation	Ontological specification			Item response variables
Instrument Development: RQ2: What are measures of ISA?	2	Questionnaire creation	Face validity check n=3		2, 5	Instrument items
	3, 4	Pre-test	Original instrument n=7	7	7	
	3, 4	Pilot test	Small sample administration n=286	7	10	
RQ3: Which information security practices reflect ISA?	3, 4	Item Screening	Lawshe procedure n=1			
	3, 4	Administer Final Questionnaire	Full administration n=531	1, 2, 3, 4, 5, 8, 9	3, 12, 13, 14, 17	
		Instrument Evaluation	CFA, EFA Scree plot Known-groups	6	4, 6, 9, 11, 15, 16	Validity assessment
			Cronbach's Alpha	6	8	Reliability assessment
Statistical Profile: RQ4: Do security practices differ between computing-environments?		ISA Profile • ISA • ISP@W • ISP@H	Factor scoring Descriptive statistics Norming data analysis SEM / MR			Profile data: • Demographic data • ISA scales • ISP@W scales • ISP@H scales
RQ5: Does CSE influence ISA?		CSE Profile	Hypothesis testing			Hypothesis retained or rejected
RQ6: Does PI influence ISA?		PI Profile				

Table 13

items. Instrument development includes identifying ISA, ISP@W, ISP@H, PI, and CSE scale items for the questionnaire, and then pre-testing, pilot testing, item screening, administration, and evaluation of the instrument.

Inherent in the first three research questions are qualitative concerns about ISA domain measures, which require well-developed survey attributes (Zmud and Boynton, 1991). Table 14 lists nine desirable survey methodological attributes (SMA) (Grover et al., 1993). These SMAs, denoted in this research as SMA-n, provide methodological standards or norms for survey research that allow replication or further research of particular study results (Grover et al., 1993). Table 15 lists 17 questions to identify ideal survey attributes (SA) that minimize measurement-related error (Malhotra and Grover, 1998). Answering each SA, denoted in this research as SA-n, reduces the survey research error (Malhotra and Grover, 1998). Combined SMA-n and SA-n addresses key success factors in survey research design for instrument development and quality improvement.

Desirable Survey Methodological Attributes (SMA-n)
(Grover, Lee, and Durand, 1993)

SMA-1. Report the approach used to randomize or select samples
SMA-2. Report a profile of the sample frame
SMA-3. Report characteristics of respondents
SMA-4. Use a combination of personal, telephone, and mail data collection
SMA-5. Append the whole or part of the questionnaire
SMA-6. Adopt a validated instrument or perform a validity or reliability analysis
SMA-7. Perform an instrument pre-test
SMA-8. Report on response rate
SMA-9. Perform a statistical test to justify the loss of data from non-respondents

Table 14

Ideal Survey Attributes (SA-n)

(Malhotra & Grover, 1998)

General

SA-1. Is the unit of analysis clearly defined for the study?
SA-2. Does the instrumentation consistently reflect that unit of analysis?
SA-3. Is the respondent(s) chosen appropriate for the research question?
SA-4. Is any form of triangulation used to cross validate results?

Measurement error

SA-5. Are multi-item variables used?
SA-6. Is content validity assessed?
SA-7. Is field-based pre-testing of measures preformed?
SA-8. Is reliability assessed?
SA-9. Is construct validity assessed?
SA-10. Is pilot data used for purifying measures or are existing validated measures adapted?
SA-11. Are confirmatory methods used?

Sampling error

SA-12. Is the sample frame defined and justified?
SA-13. Is random sampling used from the sample frame?
SA-14. Is the response rate over 20%?
SA-15. Is non-response bias estimated?

Internal validity error

SA-16. Are attempts made to establish internal validity of the findings?

Statistical conclusion error

SA-17. Is statistical power sufficient?

Table 15

Content Analysis of the ISA Literature

Content analysis involves research techniques that describe and scientifically analyze the content of written, spoken, or image communication (Churchill, 1979). Authors' observations can infer meaning about a theoretical construct under review. The social sciences commonly employ content analysis to draw inferences from text (Weber, 1985). For finding the domain of a concept, the procedure involves the objective and systematic extraction of attributes from written communication (Carney, 1972) that concludes with an analysis of the extracted parts (Budd, Thorp, and Donohew, 1967).

Content analysis, derived from the literature review, provides support for the policy, technology, and threat-context measures of ISA. The selected literature included academic and practitioner articles and books concerned with information security, and the awareness and practice of information security. The search criterions were the phrases *information security, information security awareness,* or *information security practice.* Selection of the articles and books occurred if the title or keywords of the article contained the search criterions. Databases accessed for articles and books that met the stated search criterions were AUBIECAT, ABI/Inform, EBSCO, and INFOTRAC at Auburn University. IT academic journals reviewed individually included Information Systems Research, the Journal of Management Information Systems, and MIS Quarterly. Bibliographies in the selected articles and books allowed review of related articles for further exploration of important information security concepts.

All articles used an ontological specification procedure described by Templeton and Snyder (1997). Ontology represents a specifying scheme of concepts that holistically describes some topic. For our purposes, an ontological specification can yield declarative knowledge about the user-level ISA concept. The procedure includes four steps: 1) selection of the topic area, 2) delineation or explanation of concepts that describe the overall construct, 3) transfer to a reusable medium, and 4) use of concepts in labeling source information. This procedure involves the establishment of several search attributes (refer to Figure 2 in Chapter II) related to ISA that amounted to several passes through the literature. One result was a collection of twelve ISA attributes found in the literature (refer to Table 7 in Chapter II).

The content analysis procedures subsequently elicited an operational definition of ISA. An operational definition is a description of the way researchers observe and measure a variable. Although operational definitions may be incomplete, they are important in establishing replicable criteria for generating a sample of representative survey items. Combinations of these items serve as an economical representation of the true definition of the user-level ISA concept.

Agreement of an operational definition of ISA serves three important purposes. First, the operational definition specifies the ISA domain, which satisfies RQ1. Second, it yields an understanding about the appropriate unit of analysis. Individuals perceive phenomena (i.e. ISA) and surveyed individuals should respond according to their own perceptions. Therefore, consistent with SA-1, the appropriate unit of analysis is user-level. Third, established criteria, based on the operational definition, identify occurrences of ISA and a survey instrument should replicate the identification. These criteria generate the original survey items that provide the basis for instrument development (refer to Tables 8a, 8b, 8c, 9, and 10 in Chapter II).

Instrument Development

The next methodological stage extends the domain definition of ISA into an instrument that answers RQ2 and RQ3. As the following descriptions show, the methodology for completing the instrument development stage involves several attempts to establish content validity.

Initial Questionnaire Development

During the initial questionnaire design, item response variables reflect a distinct attribute or characteristic of ISA (refer to Table 7 in Chapter II). The item responses (refer to Tables 8a, 8b, 8c, 9, 10, 11 and 12 in Chapter II) represent one respondent's perceptions about the presence of important ISA attributes derived from the literature content analysis. Hence, the questionnaire elicits a respondent's perception about the presence of a particular ISA attribute (PI, CSE, ISA, ISP@W, or ISP@H) among multiple user-level ISA concept attribute scale items. Multiple item response variables measure particular user-level ISA concept attributes.

As with the construction of the operational definition, item or scale question design considered the unit of analysis. Consistent with the operational definition of ISA, individuals respond to their perception of each item. Likert-scale response categories were: 1) not at all, 2) to a small extent, 3) average extent, 4) to a large extent, 5) with out question. For individuals who did not understand the concept of a particular ISA, ISP@W, or ISP@H question, the response category was 0) I do not understand. Three MIS faculty members evaluated the items in the initial questionnaire development stage. Based on their feedback, the edited items improved clarity, conciseness, and readability. Finally, a review of each item ensured it represented its originally intended meaning.

Pre-test of the Initial Questionnaire

Pre-testing is a trial run on a highly controlled sample to gain evidence about the empirical appropriateness of the original instrument before its final administration. This step begins the iterative process of data collection and instrument purification that continues throughout the instrument development stage.

Seven Ph.D. students and three administrative assistants comprised the pre-test respondents. As with all respondents used in the instrument development stage, pre-test subjects had basic familiarity of the ISA topic. Each pre-test respondent received an email that included the questionnaire, explained the project, and requested if he or she would review the questionnaire for clarity and/or enhancement. All subjects agreed. Participants submitted their responses via email or in writing by mail. A review of each participant's response resulted in revisions based on the feedback.

Rationale for Web-based Questionnaire

Computers have dramatically improved the process of analyzing survey research data (Shanks, 1991). Traditional survey research collects questionnaire data through paper-and-pencil administration. However, the method chosen for this dissertation was computer-assisted, self-administration. Shanks (1991) noted that computer-assisted surveys are desirable for one or more of the following reasons:

- the resulting information will be more accurate or complete;
- the entire process may be financially less expensive;
- the entire process may be faster; or
- the entire process may be so complex that it generates a computer-assisted need.

This study chose computer-assisted, self-administration of the pre-tested questionnaire for the first three reasons, and because the sampling frame of an electronic survey is restricted to members of organizations and populations who have access to computers (Kiesler and Sproull, 1986). Our survey questionnaire concerns individuals who use computers at work and at home. Therefore, a Web-based questionnaire is appropriate. However, the literature supports advantages and disadvantages to computer-assisted questionnaire administration.

Webster and Compeau (1996) suggested that computer-specific measures, captured by the computer, allow the computer to become both the object and means for measurement, and thus the measurement increases its relevance or salience. The authors also stated that by collecting measures relating to computers via computer, the salience of the computer increases, making participants pay more attention to the computer itself (Webster and Compeau, 1996). ISA, ISP@W, ISP@H, PI, and CSE are computer-specific measures that relate to computers. Therefore, computer-assisted administration should be an appropriate method for the pre-tested questionnaire.

Previous research suggests that computer-administered questionnaires introduce response effects that may increase cooperation, increase honesty, reduce social desirability, facilitate performance, increase guessing on multiple response items, and vary the range of response to scale items (Bratton and Newsted, 1995). Both increased guessing and variation in range of response are disadvantages that Bratton and Newsted (1995) attributed to entry-task bias. An entry-task is the mechanism (instructions and response presentation) with which individuals use for choosing and recording responses to specific computer-based questions. The mechanisms or entry tasks can vary depending on the software used to develop a computer-based questionnaire. Using these mechanisms, individuals responding to computer-based questions may have different levels of understanding for specific entry-tasks, which can vary a question's responses based on entry-task bias and not an individual's perception of the question.

Prior knowledge of entry-task bias during a questionnaire's computer-based development could minimize the response effect. To minimize guessing, participants must have a complete understanding of the mechanics and concepts required for questionnaire responses (Bratton and Newsted, 1995). The authors suggested possible guidelines for questionnaire responses that included selecting one choice; selecting more than one choice; unselecting a choice; and going back to a previous question to make changes. The authors also suggested that participants are less likely to read or understand instructions in a computerized format. Therefore, labeling each possible scale response rather than using an unlabeled scale with labeled end-points could minimize the variation in the range of response to scale items.

The College of Business at Auburn University provides network access to their Survey Builder, an in-house developed, Web-based tool that assists researchers in the building and administration of online surveys. The survey tool provides the capabilities to create the pre-tested questionnaire as a Web-based questionnaire, assist in survey administration, and collect the survey responses in a tabular, database format. Appendix A lists a printout of the resulting Web-based questionnaire that incorporated the response effect suggestions from Bratton and Newsted (1995).

Pilot Test of the Pre-tested Questionnaire

Pilot testing uses field-based data to evaluate or purify the pre-tested questionnaire. This procedure allows last-minute item corrections and adjustments. The purpose of the procedure is to gain experience in administering a "dry run" questionnaire version to a small sample.

An introductory email, that included an attached cover letter and the pre-tested questionnaire URL, requested the individual to participate in the pilot test. 400 business students received the introductory email. The introductory email (Appendix B) and cover letter attachment (Appendix C) explained the purpose of the research. The email directed each student to register for access to the Web-based survey, complete the Web-based questionnaire, and suggest additional ISA attributes or questionnaire administration tips. Appendix D depicts the browser screen that respondents used for survey registration. The Web-based survey design required respondents to have Internet access, email access, a Web browser, and the Web-based questionnaire URL. Respondent feedback helped further revise the pre-tested questionnaire and the questionnaire administration.

Item Screening of the Pilot Tested Questionnaire

The purpose of this step is to have experts on information security ensure that items edited in previous steps still hold their intended meaning. The procedure involves selecting an evaluation group or panel. The panel consisted of individuals who are knowledgeable about information security among desktop computer management, virus protection, and local-area-networks. Lawshe (1975) developed a quantitative procedure for assessing content validity designed to determine whether each questionnaire item adequately represents the content domain. Individual panelists would assess each of the ISA items, ISP@W items, and ISP@H items with a rating as either 1) not relevant, 2) important (but not essential), or 3) essential to the user-level ISA concept. In accordance with Lawshe, panelist responses for each questionnaire item computed a content validity ratio that follows the formula:

CVR = (n – N/2) / (N/2) where,

n is the frequency count of the number of panelists rating the item either 2 or 3

N = the total number of respondents

This procedure computes a content validity ratio (CVR) that represents a qualifying consensus for content validity of each item response variable. Should more than half, but less than all panelists state that an item response variable is essential, the respective CVR falls between zero and .99 (Lawshe, 1975). The CVR allows the elimination of item response variables based on the panelist concurrence occurring through chance. For example, a 15-member panel would require a CVR ratio of .49 or higher to retain an item response variable that satisfies a .05 level of chance occurrence.

Administer Final Version of Questionnaire

This step involved administering the questionnaire to the target sample. The target group selection preceded the introductory Web-based questionnaire email and response quality assessment.

Choosing respondents appropriate for the research questions and defining the sample respondents guided the selection of the target population as organizational computer users. Auburn University employees limited the target group. Full-time faculty, non-tenure faculty, academic and professional (A/P), and staff employees among 18 university area classifications (AAES, Administration, ACES, Architecture, Agriculture, Business, Education, Engineering, Forestry, Graduate, Honors, Human Sciences, Liberal Arts, Nursing, Outreach, Pharmacy, COSAM, Veterinary Medicine) comprised the sample. The GroupWise address book for Auburn University identified email addresses and associated job titles from organizational computer users among the 18 areas and job type classifications. The final sample consisted of Auburn University full-time employees with valid email addresses.

The introductory emails and cover letter attachment followed the Auburn University Institutional Review Board (IRB) procedures for human subject research; according to IRB protocol #05-187EP0509. Each email requested that an individual register for the survey and then access and complete the Web-based questionnaire. The selection of all full-time employees from specific university areas and job type classifications was a sample of convenience.

Different university areas received survey-participation emails at different times, which allowed for the orderly completion of questionnaires across all 18-area classifications. Comparing known-groups distributions among the completed questionnaires to the original distribution among the target population checked for non-response bias. A one-sample chi-square test assessed whether the group distribution represented by the sample respondents was statistically different from the group distribution in the population. Comparing the number of completed questionnaires to the target population that opened introductory emails also computed the questionnaire response rate.

Instrument Evaluation

Instrument evaluation addressed the psychometric properties of the instrument that included content validity, construct validity, triangulation, factorial validity, and reliability. Construct validity measures whether or not an instrument assesses what it is supposed to, or the extent to which it is free of systematic error. Reliability measures the consistency of an instrument from one sample to the next, or the extent to which it is free of random error. The assessment of 1) content (subjectively judged) and construct (empirically judged) validity and 2) reliability properties were two distinct categories of testing conducted in instrument evaluation. Statistical analysis used either the Statistical Package for the Social Sciences (SPSS) for statistical routines or AMOS statistical software for structured equation modeling (SEM). Also, statistical power analysis used GPOWER version 2.0 software.

Content validity. A measure has content validity when the scale items accurately represent the domain that requires measurement. Cronbach (1971), and later Kerlinger (1986), defined content validity as the adequacy in which scale items represent the population of items on the concept. Content validity is a statistical result, yet it is also a matter of expert judgment. In this study, the iterative refinement process prescribed by Churchill (1979) and Cronbach (1971) addressed content validity. Three Management Information Systems (MIS) faculty professors reviewed the original questionnaire draft for face validity. In the pre-test and pilot test, knowledgeable computer users reviewed the instrument. The Lawshe procedure employed information security experts to provide opinions, transformed opinions into measures, and statistically calculated the content validity for each questionnaire item. In all four procedures, qualified reviewers assessed the instrument content and refined the scale items.

Construct validity. The extent to which an instrument accurately measures the concept of interest is construct validity. Carmines and Zellar (1979) explained that construct validity is the representativeness or sampling adequacy of the construct domain. It is concerned with how a measure relates to other measures consistent with hypotheses about the theory-based construct. Construct validity tests determine whether the measure reflects true dimensions of the concept or methodological problems distort the measure (Cronbach and Meehl, 1955). Using an appropriate operational definition of the concept under review demonstrates construct validity (Stone, 1978; Kerlinger, 1986).

Several tests exist to measure construct validity, which include observing logical factors through factor analysis (Allen and Yen, 1979), known-groups analysis, and reliability tests (Kerlinger, 1986). However, the tests require triangulation to address content validity fully. Triangulation involves using two or more methods to observe or test the same phenomenon. Triangulation research strategy uses multiple methods (multivariate or univariate tests) to analyze the data. This study used triangulation to measure construct validity.

Factor Analysis. Harman (1976) suggested that factor analysis allows researchers to take a large number of variables (scale items) and reduce them to a smaller number of variables (i.e. latent variables or factors). Allen and Yen (1979) noted that the appearance of logical factors during factor analysis is an indication of construct validity. Factor analysis also provides empirical validation for grouping scale items with similar theoretical meanings (Kim and Mueller, 1982). Examining each scale item that makes up an overall logical factor is a legitimate method for assessing construct validity (Stone, 1978; Allen and Yen, 1979; Kerlinger, 1986). Therefore, this study used factor analysis as an empirical basis to distinguish items that represent ISA, ISP@W, ISP@H, PI, and CSE.

Factor analysis uses simplicity (Harman, 1976; Sethi and King, 1991), interpretability (Kachigan, 1982; Lederer and Sethi, 1992), and the percent of variance explained (Bernstein, 1988; Straub, 1989) to judge possible factor solutions. A factor solution or factor is a cluster of highly intercorrelated scale items or variables. Simplicity in factor analysis calls for the minimum number of common factors, where each variable (scale item) should load on only one common factor (Kim and Mueller, 1982). Factor analysis also involves interpreting patterns among the variations in variable clusters or groups. Interpretability relates to how well the patterns are distinguishable between the variable-to-factor loadings and variable groups. An eigenvalue is a statistic used in factor analysis to indicate how much a particular factor accounts for the variation in the original group of variables. Each empirically derived factor requires an eigenvalue greater than one (Nunnally, 1978). A scree plot graphs the eigenvalues. A scree test is a heuristic judgment made from the scree plot to determine how many factors best represent the group of variables and the associated percent of variance explained.

Theory supports ISA, ISP@W, ISP@H, PI, and CSE. However, these constructs are not present in the literature within one cohesive model. Factors derived from theory require confirmatory factor analysis. Therefore, the factor analysis used in this study involved confirmatory methods using SPSS and AMOS software to confirm the user-level ISA concept research model (refer to Figure 10 in Chapter II).

Known-groups Analysis. Known-groups analysis is a method of investigating construct validity (Cronbach and Meehl, 1955). Based on the researcher’s understanding of the construct, a hypothesis defines how groups should differ in terms of measurement. The known-groups criterion for construct validity states that construct and subscale means should differ across groups as theoretically expected. Years of computer use, job classification, hours of average weekly computer use, and hours of average weekly

Internet use are attributes that should differentiate respondents and influence ISA scale or subscale scores (see Tables 8a and 8b, Chapter II).

Reliability. Reliability is a requirement for construct validity (Nunnally, 1967). Reliability assesses the extent to which random error (i.e. variation or unreliability) exists in the instrument. Reliability occurs when repeated measures from the same instrument for the same sample give similar results. Reliability assesses the consistency of an instrument in measuring a concept across different samples. A standard procedure for assessing reliability is Cronbach's reliability coefficient alpha, a statistic ranging from 0.0 (no reliability) to 1.0 (complete reliability).

Statistical Profile

The last methodological stage further extends the domain definition of ISA and the sample data set of scale item measures that represent individual perceptions of ISA, ISP@W, ISP@H, PI, and CSE. From this sample data, scale item measures serve as the basis for developing ISA, PI, and CSE statistical profiles. Factor scores result from summing the item scores (scale item measures) for specific items that make up a given factor (Churchill, 1979). Means, standard deviations, and quartiles of factor scores may serve as a reference, or norm, for future uses of the measuring instrument (Churchill, 1979).

Basic descriptive statistics (mean and standard deviation) computed for each ISA, ISP@W, ISP@H, PI, and CSE scale item provides a detailed perspective. SPSS software provided the statistical procedures. Comparisons between basic descriptive statistics for security practice at work (ISP@W scale items) and security practice at home (ISP@H scale items) answered which security practices differed (RQ4).

Structural equation modeling (SEM) techniques that included analysis of variance (ANOVA), confirmatory factor analysis, or multiple regression (MR) provided empirical support to perform hypothesis testing from Chapter II. SPSS software provided the statistical procedures and AMOS software provided the SEM tools. Hypothesis testing applied to the following hypotheses:

H1: Higher measures of user-level ISA should positively affect user information security practice at work.

H2: Higher measures of user-level ISA should positively affect user information security practice at home.

H3: Information security practice at work, which has high measures of user-level ISA perspectives of policy and technology, should positively affect user information security practice at home.

H4: High measures of user-level PI should positively affect high measures of ISA.

H5: High measures of user-level CSE should positively affect high measures of ISA.

The results from the hypothesis test of H4 answered whether PI influences ISA (RQ5). Likewise, the results from the hypothesis test of H5 answered whether CSE influences ISA (RQ6).

Chapter Summary

The methodology employed in this research combined survey design frameworks from Churchill (1979); Grover, Lee, and Durand (1993); Lewis (1993); Malhotra and Grover (1998); and Templeton (2000). The content and construct validity tests facilitated greater internal and external validity (generalizability) of the measures (ISA, ISP@W, and ISP@H) and items (refer to Tables 8a, 8b, 8c, 9, and 10 in Chapter II). The research methodology considered all but SMA-4 from Grover et al.'s desirable survey methodological attributes. Personal, telephone, and mail data collection were not applicable with a Web-based questionnaire. The research methodology also considered all of Malhotra and Grover's ideal survey attributes, which assures that the development of quality measures for ISA, ISP@W, and ISP@H employ sufficient rigor.

CHAPTER IV. ANALYSIS OF RESULTS

Introduction

This chapter presents the study results by examining the constructs of interest (ISA, ISP@W, ISP@H, PI, CSE) that address the posed research questions and hypotheses from Chapter II, according to the methodology described in Table 13 from Chapter III. The results are organized into five sections, each dedicated to investigating the results of the methodological steps intended to answer corresponding research questions. The sections are 1) results of content analysis, 2) results of instrument development, 3) results of CFA, 4) results of hybrid model analysis, and 5) results of known-groups analysis. The latter three sections comprise portions of the instrument development and statistical profile stages from Chapter III.

Results of Content Analysis

The definition for the awareness and practice of information security was based on conclusions from the literature review (Chapter II). The definition was also based on the operationalization techniques described in the methodology (Chapter III). Therefore, the operational definition employed in this research follows.

> *The awareness and practice of information security is defined as continuous deterrent and/or preventive efforts, which have the behavioral intent to limit the loss in data utility. These continuous efforts are derived and accomplished through the identification of possible threats, assessment of known risk or cost to loss ratio, and decision to mitigate the associated risk with employment of appropriate, associated threat-context countermeasures of access control, physical protection, user authentication, security management, and encryption.*

Table 8c in Chapter II listed individual ISA measures as item-response variables, based on policy (FP or IP), technology (T), and threat-context (C) perspectives. Table 9 in Chapter II listed ISP@W practice as item-response variables that represent the employment of appropriate deterrent (D) and/or preventive (P) security efforts within the formal (business) computing-environment. Table 10 in Chapter II listed ISP@H practice as item-response variables that represent the employment of appropriate threat-context countermeasures for access control (TA), physical protection (TP), user authentication (TU), encryption (TE), and security management (TS) within the informal (home) computing-environment. Tables 8a and 8b in Chapter II respectively depict the demographic and technology variables associated with respondents in both formal and informal computing-environments. All of these measures are characteristics of ISA. These characteristics, along with the PI and CSE scales from respective Tables 11 and 12 in Chapter II, represent the content analysis results and the survey instrument in this research. In combination, these measures represent the user-level ISA concept model (refer to Figure 10 in Chapter II).

Content analysis results are the foundation from which to answer the first research question. What is the domain of information security awareness? The definition of the awareness and practice of information security and the characteristics identified in the measures of the user-level ISA concept specified the domain of information security awareness.

Results of Instrument Development

The original draft of the questionnaire from the methodological Stage 1 (Content Analysis) included 142 questions about demographics (16), CSE (16), PI (20), ISA (23), ISP@W (23), and ISP@H (44). The refinement procedures of face validity and pre-testing reduced the questionnaire to 126 questions for the pilot study and 127 questions for the final administration (refer to Appendix A). Education level was not deemed an appropriate question for the pilot study's target sample of university business students. The refinement process also generated an "I do not know" response included with the 5-point Likert scale for ISA, ISP@W, and ISP@H item responses. The intent of the added response was to distinguish between respondents who did not understand certain terms in a given question verses respondents who were not aware or did not perform a given information security practice.

Pilot study

Undergraduate business students, enrolled in an introductory MIS course during fall semester of 2005, were the pilot study sample population (286 out of 400). Students who registered and responded to the online survey yielded a response rate of 72%. The high response rate was attributed to the course professor giving extra-credit for students who completed the survey. The pilot study refined logistic concerns of administering the online survey and confirmed the need for the "I do not know" response among the ISA, ISP@W, and ISP@H items. The average "I do not know" response per question was 9%. Among the respective survey items, 32 of the 80 questions (40%) had "I do not know" responses greater than 10%. Without this response option, the "I do not know" responses could have been miss-interpreted as "not at all" and skewed the "not at all" responses beyond the average 25%. Appendix B lists the pilot study item-responses and frequencies.

Item Reliability Assessment of Pilot Study Results (n=286)

Construct	CSE	PI	ISA	ISP@W	ISP@H
Cronbach's α	.95	.88	.92	.89	.91

Table 16

Since the target population of the research was full-time university employees, the pilot study was only used to test the construct validity of item-responses through reliability statistics and known-groups analysis. Table 16 depicts the pilot study reliability assessment of CSE, PI, ISA, ISP@W, and ISP@H. All five constructs yielded reliability statistics above the desirable level of 0.80 (Nunnally, 1978). These reliability statistics encouraged full administration of the questionnaire.

Information Systems Management (ISMN) majors have potentially higher computer literacy and familiarity with information security concepts by the nature of their studies. Thus, known-groups analysis yielded differences ($p<.10$) between majors. Table 17 depicts the results for construct average mean differences between students majoring in

ISMN versus Accounting (ACCT), Marketing (MKTG), and non-specified (Other) majors. ISMN majors had higher average PI item-responses (p<.03 with .85 power). ISMN majors also showed slightly higher average ISP@W and ISP@H item-responses (p<.10 and power = .79 and .65, respectively). Known-groups validity encouraged full administration of the questionnaire.

Known-groups Differences in Pilot Study (n=286)

Construct	Majors ISMN (n=17) (I) vs. (J)	Mean Difference (I-J)	Std. Error	p-value	(I) mean	(J) mean
PI	ACCT (n=83)	.46	.14	.024	3.20	2.74
	MKTG (n=88)	.48	.14	.015	3.20	2.72
	Other (n=45)	.53	.15	.010	3.20	2.67
ISP@W	ACCT	.57	.20	.066	2.79	2.22
	MKTG	.55	.20	.084	2.79	2.24
ISP@H	MKTG	.51	.19	.090	2.83	2.32

Based on observed means. Multiple Comparisons – Tukey HSD

Table 17

Lawshe Procedure

The Lawshe procedure employed experts to provide opinions for each questionnaire item. However, ISA, ISP@W, and ISP@H item-responses were based on published formal and informal Auburn University security policies (Auburn University, 2006a), along with available university provided technologies (Auburn University, 2006b). Thus, upon conclusion of the pilot study, the pilot study results and the questionnaire were reviewed by the Auburn University Office of Information Technology (OIT). Within OIT, the Director of Campus Networking employed one individual who monitors and advises the OIT group on information security concerns and practices. The OIT Security Specialist reviewed the questionnaire and supported the item-response variables for ISA, ISP@W, and ISP@H.

Final Administration of Survey

During January 2006, 4,938 full-time employees received email requests for survey participation. Pinosonneault and Kraemer (1993) noted that inadequate sample size under 300 was a leading weakness in MIS survey research methodology. However, the number of participants desired for this study was at least 400 or over 8% of the target population.

Survey registration and respondent online submissions were conducted during January and February 2006. 3,359 full-time employees (68%) opened their email request to participate. A total of 47 separate email correspondences were received and/or made with 19 employees concerning clarifications (47%), feedback (40%), and requests for results (13%). 531 employees registered and submitted a survey response. Employees who opened the email request yielded a response rate of 16% and 11% of the target population responded.

Table 18 depicts respondent summaries from the initial 18 university areas. The combined response rate met the minimum desired sample size. However, the rate was below 20% (refer to SA-14 from Table 15 in Chapter III), which could be attributed to one or more of the following reasons. Some employees may have negative bias toward online surveys or lack interest in survey participation. The sensitive nature and/or complexity of information security may have seemed intrusive and limited employee response. The clarification that survey responses were confidential and data analysis was anonymous may not have overcome individual fear of associating email addresses with survey responses. Individual effort required to read an email, register for the survey, and access the password-protected survey may have seemed too over-whelming or complex for participation. Lastly, employee skepticism over the time required to answer 127 questions may have allowed other priorities to take precedence over survey participation. Nevertheless, the response rate was favorable compared to the 1.6% response rate experienced during the information security research of Kotulic and Clark (2004).

Information Security Survey Respondents by University Area

Group	Emails	Opened	Responses	% Response
University Administrative	**1,315**	**913**	**149**	**16.3**
Administration	1219	844	123	14.6
Graduate School	25	18	7	38.9
Honors College	3	2	0	0
University Outreach	68	49	19	38.8
Medical Sciences	**613**	**262**	**75**	**28.6**
School of Nursing	45	32	10	31.3
Harrison School of Pharmacy	143	102	16	15.7
College of Veterinary Medicine	425	128	49	38.3
Natural Sciences	**2,222**	**1,558**	**235**	**15.1**
College of Agriculture	552	390	34	8.7
Alabama Ag. Exp. Stations	69	49	8	16.3
Alabama Coop. Ext. System	610	431	74	17.2
School of Forestry/Wildlife Sciences	117	84	4	4.8
College of Architecture	76	60	0	0
Ginn College of Engineering	408	331	61	18.4
College of Human Sciences	115	82	8	9.8
College of Science & Mathematics	275	131	46	35.1
Social Sciences	**788**	**626**	**72**	**11.5**
College of Business	301	202	33	16.3
College of Education	109	84	10	11.9
College of Liberal Arts	378	340	29	8.5
Combined	**4,938**	**3,359**	**531**	**15.8**

Table 18

Non-response bias in the sample data was investigated by comparing the responses and non-responses across the target population by using a chi-square, one-sample test. Due to the lack of survey responses across all 18 university areas, the convenience sample was stratified into four super university-area groups: university administrative, medical sciences, natural sciences, and social sciences. Table 18 also depicted the aggregation of the initial 18 university areas into the four super groups. The computed chi-square statistic, testing the sample distribution against the population distribution, was 4.08 with 3 degrees of freedom. Thus at a significance level of .05, the population distribution present within the sample was not significantly different than the population distribution across the super university-area groupings.

Information Security Survey Respondents by Job Type

Job Type	Staff	A/P	NTF	Faculty	Combined
Employees	1,317	1,321	649	1,651	4,938
Survey Responses	124	220	53	134	531
% Survey Responses	9.4	16.7	8.2	8.1	10.8

Table 19

Table 19 depicts respondents by job type: staff, academic/professional (A/P), non-tenure faculty (NTF), and faculty. The A/P job type had roughly double the percentage of respondents, which could be attributed to the large percentage of information technology professionals (16%) within the job type. The computed chi-square statistic for the staff versus non-staff job types was 3.35 with 1 degree of freedom. Thus at a significance level of .05, the population distribution present within the sample was not significantly different than the population distribution between staff versus non-staff job types. Both chi-square, one-sample tests across university areas and job types suggested a lack of non-response bias among the submitted questionnaires relative to the overall target population.

Instrument Evaluation

As described in Chapter III, content and construct validity were assessed in this research. Given the rigor established during the Instrument Development Stage, the level of content validity for this instrument was adequate for empirical testing. Appendix F depicts the descriptive statistics (mean, standard deviation, minimum, maximum, skewness, and kurtosis) and Appendix G depicts the response frequencies for each item-response variable. Content validity was verified by the quantitative results found from construct validity testing.

Factor Analysis Pre-tests of Respondent Data

Item Responses	KMO	Barlett Sphericity		Skewness		Kurtosis	
		X^2	df	High	Low	High	Low
ISA	.91	5738.19	171 **	+0.09	-2.34	+5.74	-1.46
ISP@W	.87	4996.75	276 **	+1.27	-1.66	+1.83	-1.40
ISP@H	.88	7862.31	666 **	+1.56	-1.72	+2. 55	-1.58
PI	.91	5667.86	190 **	+0.83	-0.33	+0.70	-0.76
CSE	.93	5234.79	45 **	+0.04	-1.06	+0.50	-1.06

** p-value<.00

Table 20

Before construct validity could be assessed using the response data, four tests were performed to determine whether or not factor analysis was appropriate. Table 20 depicts test results from the Kaiser-Meyer-Olin (KMO) test, Bartlett sphericity test, skewness test, and kurtosis test for ISA, ISP@W, ISP@H, PI, and CSE item-responses. The KMO statistics exceeded .80 or the meritorious range and three sets of item-responses (ISA, PI, and CSE) exceeded .90, which is in the marvelous range (Hair, Anderson, Tatham, and Black, 1995). The Bartlett statistics were significant at the p<.00 level. Skewness and kurtosis statistics fell within the ±3 and ±10 ranges respectively, where deviations would have indicated potential non-normality problems associated with extreme skewness or kurtosis (Kline, 1998). Thus, the sets of item-responses are amenable to factor analysis.

Results of Confirmatory Factor Analysis

Confirmatory factor analysis of the ISA, ISP@W, ISP@H, PI, and CSE item-responses provided answers to the second, third, and fourth research questions, as well as supporting the content analysis answer for the first research question. By forcing item-responses to load solely on an *a priori* construct, individual constructs confirmed their contribution to explained item-response variable variance (squared multiple correlations or SMC). An item-response variable was retained if the standardized regression weight (SRW) was significant (p<.05) and SRW absolute value was .50 or higher (Kline, 1998). Each retained item had a respective construct that explained at least 25% of the item-response variance (SMC).

The power (Cohen, 1977) of the CFA retain criteria test was 1.00 (based on N = 531, α = .05, and SMC = .25). Furthermore, with the sample size of 531 and α = .05, a .96 power existed for the SMC or R^2 = .03. However, the power was .84 for the SMC or R^2 = .02. The CFA had substantially reduced power distinguishing extremely small associations (α = .05 and SMC or adjusted R^2 < .02).

The completed CFA consisted of two sequenced iterations. The first iteration identified item-response variables that did or did not meet the retain criteria. The second iteration used the ISA domain measures (RQ1) as respective item-subscales for the retained ISA, ISP@W, and ISP@H items. The CFA model goodness-of-fit statistics from both iterations gave credibility to within and between construct reviews of retained individual traits, awareness, and practices.

From the initial CFA iteration, all CSE items were retained. However, 3 ISA items, 13 ISP@W items, and 22 ISP@H items were dropped due to low SRW (weak relationships). Furthermore, non-significant or low SRWs also rejected six and dropped three PI items, respectively. Item-response variables for PI, ISA, ISP@W, and ISP@H that were dropped or rejected from further SEM analysis are listed in Tables 21, 22, 23, and 24 respectively. Seeking explanations for the weaker or stronger PI, ISA, ISP@W, ISP@H relationships further defined the constructs under review. The remainder of the section reviews the CFA model goodness-of-fit, rejected or dropped item-response variables, item subscales substitution for item-response variables, and retained ISA, ISP@W, and ISP@H item-response variables. The section concludes with estimated parameters from the second CFA iteration, all of which supported answers to RQ1, RQ2, RQ3, and RQ4.

CFA Model Fit

Appendix H depicts the second iteration CFA model where exogenous variables ISA, ISP@W, ISP@H, PI, CSE, and unconstrained SEM error terms were correlated. Endogenous, observed item-responses and constrained error terms explained respective relationships among the exogenous variables. Kline (1998) noted that SEM goodness-of-fit indices reflected different facets of model fit and a minimal set should include the X^2 statistic with degrees of freedom, overall proportion indexes, and an index for the residuals. The recursive and identified CFA model was an adequate, representative fit for the 531 item-responses, as indicated by the supporting goodness-of-fit statistics: CMIN/DF, GFI, CFI, RMR, SRMR, and RMSEA. The following discussions present the respective goodness-of-fit statistic in context to the second iteration CFA model (refer to Appendix H). For reference, the first iteration CFA statistics were also noted within the respective discussions.

CMIN/DF: minimum discrepancy / degrees of freedom. CMIN or minimum discrepancy, presented as a X^2 statistic, represented the estimated differences between the sample and the target population covariance matrix. However, the large sample sizes required by SEM magnify the significance of even slight differences. The CMIN for the default model in the first iteration was 9021.55 ($p<.00$) and 972.73 ($p<.00$) for the second iteration. DF or degrees of freedom for the default model was 5637 in the first iteration and 430 in the second. The X^2 statistic divided by the degrees of freedom reduced sample size sensitivity (Bollen, 1989) and the ratio should be less than 3 (Kline, 1998). CMIN/DF for the first iteration was 1.60 and 2.26 for the second.

GFI: Jöreskog-Sörbom Goodness of Fit Index. The GFI indicated the proportion of the observed covariances explained by the model-implied covariances. Index values that indicate proportions of observed covariances should be .90 or greater (Kline, 1998). The GFI of the first iteration was .64 and .90 for the second iteration.

CFI: Bentler Comparative Fit Index. A comparative fit between the hypothesized (default) model and the independence model explained the CFI, a proportional index that also accounts for sample size (Kline, 1998). A cutoff value of .95 or greater was advised for an adequate fit (Byrne, 2001). The CFI of the first iteration was .83 and .96 for the second.

RMR: root mean square residual. RMR provides an overall summary of the magnitude in discrepancies between the observed and model-implied covariance residuals (Marcoulides and Hershberger, 1997). However, the magnitude of RMR was also dependent on the scaling of item-responses, which required standardization. The RMR of the first iteration was .16 and .07 from the second.

SRMR: standardized root mean square residual. The SRMR was a standardized summary of the average covariance residuals, or differences between the observed and model-implied correlation matrices (Bollen, 1989). An increase in the average discrepancy increased SRMR. Kline (1998) noted that the absolute values of correlation residuals were favored at .10 or less. However, Byrne (2001) noted that in well-fitting models this statistic was small (.05 or less). The SRMR of the first iteration was .09 and .06 from the second.

RMSEA: root mean square error of approximation. Byrne (2001) noted that RMSEA was recognized as one of the most informative criteria in covariance structure modeling. RMSEA accounted for errors of approximation within the covariance matrix, given the availability for optimally chosen, unknown parameters. RMSEA also accounted for model complexity based on the number of estimated parameters. AMOS software calculated a 90% confidence interval for the estimated RMSEA range and a closeness of fit test that questioned whether the hypothesized RMSEA was “good” in the population.

Byrne (2001) noted that an RMSEA of .08 or less indicated reasonable errors of approximation and less than .05 indicated good fit. A p-value greater than .5 from the closeness of fit test indicated that the RMSEA was "good" in the population. The RMSEA of the first iteration (p<1.00) was .046, which yielded a 90% confidence interval between .044 and .048. The RMSEA of the second iteration (p<.68) was 0.049, which yielded a 90% confidence interval between .045 and .053. The 90% confidence interval for each CFA iteration overlapped. Also, both CFA iterations retained the hypothesis that the RMSEA was "good" in the population. Therefore, RMSEAs from both iterations yielded adequate fits between the CFA model and the item-responses.

Dropped PI Item-response Variables

Dropped PI Item-response Variables

SRW	Item-response Variable	p-value
.13	PI04...I am generally cautious about accepting new ideas.	**.03**
.29	PI06...I am suspicious of new ways of thinking.	**.00**
.08	PI07...I rarely trust new ideas until I can see whether the vast majority of people around me accept them.	.22
-.04	PI10...I am usually one of the last people in my peer group to accept something new.	.56
.11	PI13...I am reluctant about adopting new ways of doing things until I see them working for people around me.	.08
.03	PI15...I tend to feel that the old way of living and doing things is the best way.	.58
.46	PI16...I am challenged by ambiguities and unsolved problems.	**.00**
-.12	PI17...I must see other people using new technologies before I will consider them.	.06
.10	PI20...I often find myself skeptical of new ideas and practices.	.09

Table 21

Table 21 lists the nine PI items that were dropped for non-significant relationships (six items) and low SRWs (three items). The six rejected (p>.05) PI items correspond to specific concepts that classified respondents as late majority or laggards (Hurt et al., 1977). In reviewing the descriptive statistics (Appendix F) and frequencies (Appendix

G), the majority of respondents used the "not at all" or "to a small extent" response for these items. Conversely, the retained PI items corresponded with concepts that classified respondents as innovators, early adopters, and early majority.

Low SRWs. Two dropped items (PI04 and PI06) had weaker PI relationships. One dropped PI item (PI16) was close to meeting the retain criteria, with 73% of the respondents clustering to an average extent or better. However, a retained item (PI19) reflected a similar, associated concept ($R^2 = .38$ at p<.00).

Over all, the initial 20 PI items had a reliability (Cronbach's alpha) of .84, the nine rejected or dropped PI items had a reliability of .83, and the 11 retained PI items yielded a reliability of .92. Therefore, CFA refined the reliability of PI item-responses with respect to our hypothesized model.

Dropped ISA Item-response Variables

All three dropped, policy items from Table 22 confirmed *a priori* positive ISA relationships (refer to Table 8c in Chapter II). Each item's ISA relationship explained variance. However, other items had stronger ISA relationships and explained more variance. Lack of respondent understanding was observed among two of the three weaker ISA relationships.

Dropped ISA Item-response Variables

SRW	Item-response Variable	p-value
.46	A05...that it is a good idea to keep my passwords safeguarded.	.00
.43	A07...that the Auburn University Office of Information Technology offers virtual private network (VPN) software for use outside of the on-campus intranet.	.00
.47	A08...that the Auburn University virus protection policy requires the restriction or quarantine of computers with viruses.	.00

Table 22

Item A05. A retained, threat-context item (A13) had a similar, associated (R^2 = .38 at p<.00) concept to the dropped, policy item (A05). Appendix G showed, to a large extent or better, that over four out of five respondents (85%) knew about item A05. In fact, over three out of five respondents (70% from Appendix G) knew without question that safeguarding passwords was a good idea (A05). Item A05 yielded the highest positive kurtosis (5.74) of all item-responses (refer to Table 19). However, over four out of five respondents (89%) knew password secrecy was fundamental (A13). Therefore, password confidentiality awareness (A13) beyond security policy (A05) yielded the stronger ISA relationship.

Item A07. Respondents did not completely understand the VPN concept in item A07, which potentially yielded a weaker ISA relationship. Frequency results show that about two out of ten (22%) respondents knew without question the policy for VPN software availability (A07). Yet, five out of ten respondents (52%) did not understand the VPN concept (24%) or had less than average awareness about the software availability (28%). Also, a retained, threat-context item (A18) had a similar, associated (R^2 = .10 at p<.00) concept to the policy item (A07). Thus, encryption awareness had the stronger ISA relationship over VPN security policy.

Item A08. Another retained, policy item (A06) was a similar, associated (R^2 = .21 at p<.00) concept to item A08. From the results, over one out of four respondents (26%) knew without question the policy of quarantining virus-infected computers (A08) and the majority of respondents (58%) were aware on average or better. However, policy item A06 provided higher deterrent certainty awareness against virus infection (79% on average or better). Item A06 had the stronger ISA relationship versus high deterrent severity awareness on the results of virus infection (A08). As previously noted in Chapter II, Kankanhalli et al. (2003) also noted that deterrent certainty efforts influenced information security in lieu of deterrent severity. Exclusion of item A08 provided discriminate validity between deterrent certainty and deterrent severity awareness.

Dropped ISA items summary. The reliability statistic (Cronbach's alpha) of the 16 retained ISA items remained .91. Therefore, CFA filtered the ISA construct for redundancy (A05), lack of respondent understanding (A07), and deterrent severity awareness (A08).

Dropped ISP@W Item-response Variables

Dropped ISP@W Item-response Variables

SRW	Item-response Variable	p-value
.14	W01...I log off when I leave a computer system.	.03
.45	W02...I shut down and power-off when leaving a computer system.	.00
.19	W03...all of my computer sessions require entering a unique user-id and password combination.	.00
.46	W05...I test the restorability of back-up files that I have created.	.00
.19	W07...I rely on university provided virus protection software and its updates.	.00
.49	W11...as I surf the Web, I allow my Web browser to accept cookies from Web sites.	.00
.46	W12...as I surf the Web, I allow my Web browser to download software as deemed necessary.	.00
.43	W13...I allow software to save user-ids and passwords for faster access on return visits.	.00
.36	W17...I open emails regardless of knowing the sender's identity.	.00
.29	W20...other people share the computer(s) I routinely use that has (have) Internet access.	.00
.44	W21...viruses affect the performance of my computer.	.00
.47	W22...virus protection software has identified and limited virus impact to my computer.	.00
.41	W24...I use a character sequence like Ij4Gf4Se%f# as my computer password.	.00

Table 23

All 13 items listed in Table 23 confirmed *a priori* relationships with ISP@W (refer to Table 9 in Chapter II). The weaker ISP@W relationships, noted by CFA, were explained by examination of each item's descriptive statistics (Appendix F), response frequencies (Appendix G), and the practice within the context of the formal environment. The dropped ISP@W items were categorized by security policy obedience, security policy contradictions, risky information security practice, and trade-off practice.

Security policy obedience (Items W01, W03, and W07). Three ISP@W preventive practices (W01, W03 and W07) were grounded in formal security policy as core components. Therefore, all three items were combined deterrent-preventive practices and represented information security obedience (Thomson and von Solms, 2005).

Appendix F shows that the means of these item-responses were a standard deviation above all 11 retained item-responses. To an average extent or better, the majority of respondents conformed individual computing behavior to policy. Over four out of five respondents (86%, 86%, and 84% respectively) reported logging off when leaving a computer system (W01) where all computer sessions required a unique user-id and password combination (W03) using university supplied virus protection software (W07). However, these highly practiced, deterrent-preventive practices failed the SRW retain criteria. Other deterrent and/or preventive items (i.e. the 11 retained ISP@W items) provided better distinction of the ISP@W construct.

Security policy contradictions (Items W02, W21, and W24). Three formal practices were contradictory to security policies and the majority of respondents reported a lack of the practice to an average extent or better. 1) Powering down a computer when not in use (W02) was the ultimate preventive effort, yet less than one out of three respondents (29%) reported the practice. Informal and formal security policies in the work environment explained this lack-of-practice because computers were required to be powered-on for pushed and/or pulled software updates. 2) Also, formal security policy enlisted virus protection software as a deterrent-preventive effort to limit virus infection. So, less than two out of five respondents (37%) noted that viruses affected their computer's performance (W21). 3) Lastly, using rigorous passwords should increase information security as a deterrent effort; yet formal security policy limited password length and password content to alpha-numeric characters. Hence, less than one out of three respondents (31%) used a password like Ij4Gf4Se%f# (W24). Therefore, ISP@W deterrent-preventive items that were contrary to policy resulted in the absence of respondent practice. Furthermore, all practices that were security policy contradictions had weaker ISP@W relationships.

Risky information security practice (Items W12, W13, W17, and W20). Four practices (W12, W13, W17, and W20) were considered information security risks. Across the four practices, an *a priori* lack-of-practice was observed by respondents reporting "to a small extent" or "not at all" item-responses. 1) As an example, allowing Internet browsers to choose what software to download (W12) could be viewed as an information security risk, so over two out of five (46%) respondents reported a lack of the formal practice. 2) Allowing software to save user-id and password combinations (W13) was a convenience versus information security trade-off and over three out of five (75%) respondents reportedly chose information security via lack-of-practice. 3) Opening emails from unknown senders (W17) could be an information security risk, and over four out of five (81%) respondents reported the lack-of-practice. 4) Lastly, routinely sharing an Internet access computer with others (W20) could be an information security risk, but over two out of five respondents (53%) reported the lack-of-practice. Therefore, deterrent and/or preventive items that added information security risk resulted in the absence of respondent formal practice. These risky practices had weaker ISP@W relationships than the retained practices, and the weaker practice exclusion of CFA supported discriminate validity for ISP@W.

Trade-off practice (Items W05, W11, and W22). Three items (W05, W11, and W22) were close to the retain criteria (<.03 on average), yet respondents reported a high absence of formal practice and/or lack of respondent understanding, resulting in other IPS@W items having stronger relationships. For example, testing the reliability of data back-ups (W05) could reduce information security risk as a preventive measure, yet 32% responded with the "not at all" item-response indicating a complete absence of practice. In contrast, data back-ups on reliable media (W04), a retained preventive practice, had almost half the complete absence of practice (19%). Roughly one out of eight respondents, who reported the formal practice of data back-ups on reliable media, did not test the reliability of the data back-up. Data back-ups on reliable media had the stronger ISA relationship than testing a data back-up for reliability.

Lack of concept understanding influenced items W11 and W22 to a small extent or better. As an example, knowing when and where to allow Web browsers to accept cookies (W11) could limit information security risk and over three out of five respondents (67%) reported the formal practice. However, one out of five respondents (20%) did not understand the concept. Also, individual experience with how virus protection software had identified and limited virus impact to computers (W22) could reinforce the original decision to mitigate the associated information risk. Frequency results showed that over three out of five respondents (69%) reported the formal practice, yet one out of five respondents (20%) did not understand the concept. Lack of respondent understanding for concepts within these preventive items (W11 and W22) potentially weakened each ISP@W relationship.

Items W11 and W22 were paired with two retained ISP@W preventive practices (W06 and W08) that did not have the observed “I do not know” responses. The paired dropped versus retained items (W06↔W11 and W08↔W22) were correlated (.28 and .34 respectively at p< .00) and associated (R^2=.10 and .13 respectively at p<.00). Therefore, enabling and updating virus protection software (W06) had a stronger ISP@W relationship than knowing when and where to allow Web browsers to accept cookies (W11). Furthermore, seeking new versions of virus protection software (W08) had a stronger ISP@W relationship than individual experience with how virus protection software had identified and limited virus impact (W22). Overall, W11 and W22 had weaker relationships than other associated preventive ISP@W items without a lack of respondent understanding.

Dropped ISP@W Summary. CFA identified eleven ISP@W measures with weak relationships because similar practice measures had stronger relationships, lack of respondent practice for risky or security policy contradictions, and/or lack of respondent understanding. Over all, the initial twenty-four ISP@W items had a reliability statistic (Cronbach’s alpha) of .88 and the 13 retained items yielded a reliability of .87. Therefore, CFA maintained an approximate reliability (.87≈.88) of ISP@W item-responses while refining the construct by a 46% reduction in item-response variables that individually explained less than 25% of the total ISP@W variance.

Dropped ISP@H Item-response Variables

Dropped ISP@H Item-response Variables

SRW	Item-response Variable	p-value
.29	H01...I log off when I leave a computer system.	.00
.23	H02...I shut down and power-off when leaving a computer system.	.00
.35	H03...all of my computer sessions require entering a unique user-id and password combination.	.00
.49	H05...I test the restorability of back-up files that I have created.	.00
.48	H06...I check that my virus protection software is enabled and updated.	.00
.34	H07...I rely on university provided virus protection software.	.00
.41	H12...as I surf the Web, I allow my Web browser to download software as deemed necessary.	.00
.43	H16...I open emails regardless of knowing the sender's identity.	.00
.32	H19...other people share my computer(s) that have Internet access.	.00
.31	H20...viruses affect the performance of my computer.	.00
.36	H23...I use a surge protector and / or an uninterruptible power supply (UPS).	.00
.45	H24...all wired or wireless access to the Internet is password protected.	.00
.41	H26...I allow unknown users to access my computer files through the Internet (i.e. music, file sharing, personal Web Server, etc.).	.00
.14	H27...I try to use the same password(s) for convenience.	.03
.48	H29...I use a spam filter on my email account(s).	.00
.39	H30...I have virus protection software on my off-on-campus computer.	.00
.34	H31...I have shared devices (files, folders, drives, or printers) that are not password protected or user restricted.	.00
.49	H32...I have other computer systems or appliances that share an Internet connection.	.00
.49	H33...I have a personal firewall on my off-campus computer.	.00
.34	H34...other people know my password(s).	.00
.24	H36...I turn off or disconnect my Internet connection(s) when not in use.	.00
.46	H37...I share information security concerns with other people that share my computer systems or Internet access.	.00

Table 24

All 22 items listed in Table 24 confirmed *a priori* relationships with ISP@H (refer to Table 10 in Chapter II). Ten of the dropped ISP@H items (H01, H02, H03, H05, H07, H12, H16, H19, H20, and H27) corresponded to identically dropped ISP@W measures (W01, W02, W03, W05, W07, W12, W17, W20, W21, and W13, respectively). Three dropped ISP@H measures (H24, H36, and H37) were associated (R^2 = .06, .07, and .11

respectively at p<.00) with three other dropped ISP@H measures (H02, H03, and H19, respectively). So, identical and associated practice allowed for concurrent validity tests between and within constructs. The weak ISP@H relationships noted by CFA were explained through a comparison of each item's descriptive statistics (Appendix F), response frequencies (Appendix G), corresponding dropped ISP@W items, and the practice context within the informal environment. The dropped ISP@H items were categorized by risky information security practice, low respondent practice, high respondent practice, and trade-off practice.

Risky information security practice (Items H12, H16, H19, H26, H27, H31, and H34). Seven ISP@H items were associated with information security risks, so an a priori lack-of-practice was observed over "to a small extent" or "not at all" item-responses. Exclusion of all these risky practice measures supported discriminate validity for ISP@H.

Four of the risky practice measures (H12, H16, H19, and H27) were identical concepts to previously described risky practice that were dropped from ISP@W (W12, W17, W20, and W13, respectively). A paired t-test (p<.00) confirmed the correlation (.56, .58, .25, and .13 respectively) between the pairs (W12↔H12, W17↔H16, W20↔H19, and W13↔H27). The paired t-test supported concurrent validity between risky ISP@W and ISP@H practice.

Also, Item-responses were inconsistent among some ISP@H and ISP@W risky practice measures. The access control pairs (W12↔H12, W17↔H16, and W20↔H19) had no mean differences (p<.05). Yet, the user authentication pair (W13↔H27) had mean differences (p<.00). The information security versus password convenience trade-off was inconsistent between item-responses W13 (ISP@W) and H27 (ISP@H).

A one-sample t-test of mean differences (d=1.46 at p<.00) showed that the user authentication risky informal practice (H27) was over one S.D. higher than the mean (refer to Appendix F) of the user authentication risky formal practice (W13). Therefore, respondents were more likely to choose password convenience versus information security in the informal environment.

The three risky items, unique to ISP@H, offered additional perspectives of access control (H26 and H31) and user authentication (H34) risky practice. 1) Allowing unknown users to access computer files (i.e. music, file sharing, personal Web Server, etc.) through the Internet (H26) could be viewed as access control risk. Over three out of four respondents (78%) reported a lack-of-practice. 2) Shared devices (files, folders, drives, or printers) that are not password protected or user restricted (H31) could also be viewed as an access control risk. Two out of four respondents (54%) reported a lack-of-practice. 3) Other people knowing your password (H34) could be viewed as user authentication risk. Over three out of four respondents (82%) reported a lack-of-practice. Therefore, risky practice measures that were unique to ISP@H also resulted in respondent lack-of-practice.

In summary, risky ISP@W practice were viewed as risky ISP@H practice, both of which resulted in respondent lack-of-practice. Hence, risky ISP@H practice had weak relationships due to high respondent lack-of-practice. Furthermore, item responses for risky access control practice were consistent over ISP@W and ISP@H. Therefore, user authentication risky practice (i.e. password convenience) was higher in ISP@H versus ISP@W.

Low respondent practice (Items H01, H02, H07, H20, H36, and H37). Six ISP@H items with *a priori* positive relationships had item-responses indicating respondent lack-of-practice. Four of these items were paired to identical ISP@W practice and two items were paired with associated ISP@H lack-of-practice items. A paired t-test yielded four of the six practice pairings (W02↔H02, W21↔H20, H02↔H36, and H19↔ H37) were correlated (.28, .44, .37, and .34, respectively at p<.00), which also provided concurrent validity between constructs and within the construct.

Concurrent validity within the ISP@H construct was supported by correlation between the two ISP@H paired practice measures (H02↔ H36 and H19↔ H37) that had no mean differences (p<.05). For example, the lack of practice for shutting down and powering off when leaving a computer system (H02) correlated with the lack of turning off or disconnecting the Internet when not in use (H36). Also, the lack of sharing Internet access computer(s) with others (H19) correlated with the lack of sharing information security concerns with other people (H37). Therefore, these observed lack-of-practice item-responses were consistent over access control (H02, H19, and H36) and security management (H37) practice.

The other two correlated paired ISP@W↔ISP@H practice measures (W02↔H02 and W21↔H20) had mean differences (p<.00), which indicated inconsistent responses between environments. A one sample t-test showed that access control response means (H02 and H20) were higher (.60 and .23 respectively at p<.00) in the informal environment. These results suggested that, in the absence of security policies for powering off computers and using virus protection software, respondents powered off computers and experienced virus infections more in the informal environment. However, both access control practice measures were unassociated (adjusted R^2 = .00, p-value = .19). Furthermore, the evidence of correlation between practice measures provided concurrent validity between the ISP@W and ISP@H constructs.

The two uncorrelated, identical ISP@W-ISP@H paired practice measures (W01-H01 and W07-H07) had mean differences (p<.05), which indicated differing frequencies of practice between environments. A one-sample t-test showed that mean differences were lower (-1.3 and -1.6 respectively at p<.00) in the informal environment. The lower user authentication (H01) and access control (H07) practice measures were explained by the absence of security policy. As previously noted, a large majority of respondents (four out of five) adhered to policy governing the ISP@W practice measures (W01 and W07). Yet, the formal policies were absent from ISP@H. To a small extent or less, over two out of five respondents (43% and 55% respectively) reported a lack-of-practice for logging off the computer (H01) and relying on university provided virus protection software and updates (H07). Although both practice measures had weak ISP@H relationships, these results suggested that security policy enforced the ISP@W practice.

High respondent practice (Items H03, H23, H24, and H30). To an average extent or better, respondents reported frequent practice of a physical protection item (H23) and access control item (H30), yet both items failed the SRW retain criteria. Over four out of five respondents (84% and 91% respectively) acknowledged using a surge protector and/or uninterruptible power supply (H23) with computers having virus protection software (H30). Appendix F shows the means of these item-responses. A one sample t-test comparison of means showed that practice H23 had a higher (p<.00) mean than the retained physical protection practice (H04). A similar t-test showed that item H30 had a higher (p<.00) mean than the six retained access control practice measures (H10, H11, H13, H14, H15, and H21). However, since the vast majority of respondents conformed to these practice measures, other retained items provided better distinction of the ISP@H construct. Therefore, CFA dropped these two informal practice measures.

Two ISP@H items (H03 and H24) with *a priori* positive relationships had item-responses indicating a majority of respondent practice, yet the items also failed the retain criteria. Item H03 was identical to an ISP@W practice (W03) and was associated (R^2 = .13 at p<.00) with item H24. A paired t-test (p<.05) found one correlated practice pairing (H03↔H24 = .44 at p<.00) with no mean difference (p<.05) and one uncorrelated practice (W03-H03) with mean differences (p<.00).

The correlated paired practice measures (H03↔H24), with no mean differences, supported concurrent validity within ISP@H. Requiring computer sessions to use unique user-id and password combinations (H03) correlated with all wired and wireless access to the Internet being password protected (H24). Also, a paired t-test showed that item-responses were consistent over the respective access control practice. However, both access control items had weaker relationships than other retained ISP@H measures.

The uncorrelated, paired access control measures (W03-H03) had mean differences, which suggested inconsistent or differing practice between environments for computer sessions that required unique user-id and password combinations. A one-sample t-test of mean differences (d=-1.25 at p<0.00) found that H03 item-responses were .89 S.D. lower than the average mean item-response of W03. The formal environment had security policy that enforced the practice, yet the informal environment lacked the policy.

Therefore, the inconsistency between the ISP@W and ISP@H access control practice measures (W03-H03) was explained by the lack of security policy.

Trade-off practice (Items H05, H06, H29, H32, and H33). Five items (H05, H06, H29, H32, and H33) were close to the retain criteria (<.01 on average). Furthermore, the practice measures were either identical to or associated with other retained measures. H05 was identical to the dropped ISP@W practice of testing the reliability of a data back-up (W05), where both H05 and W05 were associated (R^2 = .55 and .51 respectively at p<.00) with the retained ISP@H and ISP@W practice of a data back-up on reliable media (H04 and W04). H06 was identical to retained ISP@W item-response W06. H29 was associated (R^2 = .04 at p<.00) with retained practice H15. H32 was associated (R^2 = .13 at p<.00) with retained practice H14. H33 was associated (R^2 = .45 at p<.00) with retained practice H10. The paired responses (W05↔H05, W06↔H06, H29↔H15, H32↔H14, and H33↔H10) were correlated (.63, .36, .20, .36, and .67 respectively at p<.00), which indicated concurrent validity between and within constructs. However, all five dropped measures had weaker ISP@H relationships with the following explanations.

Approximately two out of three respondents (63% and 64%, respectively) ascribed to testing the reliability of data back-ups within formal (W05) and informal (H05) environments. A paired-sample t-test between the measures (W05↔H05) showed no mean difference (p-value = .74) between the associated (R^2 = .40 at p<.00) preventive and physical protection practice measures. However, in both environments, CFA identified a data back-up on reliable media (W04 and H04) had the stronger ISP@W and ISP@H relationship.

A one-sample t-test between H06 and the retained ISP@H item-responses showed lower mean difference (d=-1.23 on average at p<.00) for all retained items, as evidenced where almost three out of four respondents (74%) ascribed to enabling and updating virus protection software. However, lower frequency of practice among the other retained items explained more of the ISP@H variance than this particular security management practice measure.

To an average extent or better, over one out of two (58%) respondents ascribed to using personal firewall software (H33). A one-sample t-test between H33 and the retained ISP@H item-responses showed higher (.33 on average at p<.00) and lower (-.69 on average at p<.02) mean differences, which indicated that respondents ascribed to retained ISP@H practice more and less often than H33. In fact, over one out of two respondents (52%) reported that personal firewall software monitored network traffic into/out of their computers (H10), which had a lower (-.23 p<.00) mean difference. However, almost one out of five respondents (19%) did not understand the personal firewall concept in both H10 and H33 item-responses. Yet, H10 was retained in lieu of H33 because of a stronger ISP@H relationship. Therefore, CFA dropped the redundant access control practice that explained less ISP@H variance.

To an average extent or better, over three out of five (65%) respondents ascribed to using an email spam filter (H29). Yet, over one out of five respondents (27%) reported that they stored emails on their computer rather than the email server (H15). Both items dealt with email, but H15 was retained over H29 because of a stronger ISP@H relationship. H15 resulted in a lower (-1.15 p<.00) mean difference, when compared to H29. Therefore, CFA retained the seldom practiced access control measure (H15), which explained more ISP@H variance than the frequently practiced security management measure (H29).

To an average extent or better, over one out of three (36%) respondents ascribed to having other computer systems or appliances that share an Internet connection (H32). Yet, less than one out of three (29%) respondents reported that they used file transfer software to securely move files between computers (H14). Also, H14 had a lower mean difference (d=-.20 and p<.01), when compared to H32. Both measures dealt with access control, but H14 was retained over H32 because of the stronger ISP@H relationship. Therefore, CFA retained the access control measure that explained more ISP@H variance.

Dropped ISP@H Summary. Similar measures with stronger ISP@H relationships, high respondent practice, lack of respondent practice, and/or lack of respondent understanding were attributed to measures with weak ISP@H relationships. Over all, the initial thirty-seven ISP@H measures had a reliability statistic (Cronbach's alpha) of .90 and the 15 retained measures yielded a reliability of .87. Therefore, CFA maintained an approximate reliability (.87≈.90) while refining ISP@H by a 59% reduction in practice measures that individually explained less than 25% of the total ISP@H variance.

ISA, ISP@W, and ISP@H Item Subscales

Based on ISA domain measures from the first research question (RQ1), mathematical averages of similar, retained item-responses among the ISA domain measures formed *a priori* construct item subscales. Initial iteration CFA statistics yielded SEM item subscales reliability ($\rho_{subscales}$), which allowed estimation of item subscales error variance for consistency during the second CFA iteration. The following explanations describe the domain item subscales, *a priori* confirmation, and error variance estimation.

ISA item subscales. The individual ISA measures were aggregated into technology (T), threat-context (C), and policy (P) item subscales. Respectively, Tables 25a, 25b, and 25c listed the retained ISA item-response variables by item subscales. Each table also lists the corresponding SEM regression weights (RW), SRWs, and item-response error variances (Err σ^2) from the initial CFA iteration.

ISA Technology (T) Item Subscales

Retained ISA Item-response Variables (Cronbach α = .76)	RW	SRW	Err σ^2
A01...that virus protection software can identify and remove known viruses.	0.77	0.54	0.81
A02...that virus protection software requires frequent updates.	0.84	0.59	0.74
A03...that firewall software can block network attacks.	1.31	0.65	1.36
A04...that personal firewall software can block logical port access to/from a computer.	1.30	0.58	1.92

Table 25a

ISA Threat-context (C) Item Subscales

Retained ISA Item-response Variables (Cronbach α = .90)	RW	SRW	Err σ^2
A11...that as a computer user, my knowledge of computer threats plays a significant role.	1.00	0.59	1.05
A12...that a current, restorable data back-up is necessary.	1.19	0.65	1.12
A13...that password secrecy is fundamental.	1.02	0.67	0.74
A14...of the impact that a virus can have on my computer system.	1.05	0.68	0.74
A15...of the impact that spyware or adware can have on my computer system.	1.09	0.68	0.80
A16...of the impact network attacks can have on my computer system.	1.34	0.72	0.95
A17...of the vulnerability associated with shared devices such as files, drives, or printers.	1.32	0.70	1.04
A18...that encryption can deter unauthorized access to sensitive information (i.e. credit card numbers, social security numbers, confidential emails and documents).	1.45	0.67	1.45
A19...that software requires periodic decisions and updates.	1.16	0.70	0.80

Table 25b

ISA Policy (P) Item Subscales

Retained ISA Item-response Variables (Cronbach α = .71)	RW	SRW	Err σ^2
A06...that the Auburn University virus protection policy requires use of available software and updates.	1.12	0.50	2.15
A09...that the Auburn University acceptable use policy dictates that wired and wireless network access requires an user-id and password.	1.12	0.50	2.14
A10...that other users have suggested that computer viruses can infect emails or email attachments.	1.03	0.57	1.28

Table 25c

ISP@W item subscales. Retained ISP@W measures were aggregated into deterrent (DE), preventive (PE), and combined deterrent-preventive (DP) item subscales. The combined item subscales included practice that was both deterrent and preventive security efforts. The DP item subscales were preventive practices, which were identified and/or specified from within security policies. Respectively, Tables 26a, 26b, and 26c list the retained ISP@W measures and statistics for the corresponding item subscales.

ISP@W Deterrent (DE) Item Subscales

Retained ISP@W Item-response Variables	RW	SRW	Err σ^2
W23...I routinely choose to change my password(s).	0.73	0.57	0.92

Table 26a

ISP@W Preventive (PE) Item Subscales

Retained ISP@W Item-response Variables (Cronbach α = .75)	RW	SRW	Err σ^2
W04...I back-up my data on reliable media (disks, CDs).	0.87	0.56	1.34
W10...personal firewall software monitors network traffic into/out of my computer(s).	1.12	0.63	1.62
W14...I remotely connect to other computers and share drives, printers, or files.	0.87	0.62	0.99
W15...I use file transfer software to securely move files between computers.	0.98	0.71	0.78
W18...I encrypt confidential files with passwords.	0.91	0.60	1.22
W19...I look for "https://" before I make financial transactions over the Internet.	0.99	0.53	2.12

Table 26b

ISP@W Combined (DP) Item Subscales

Retained ISP@W Item-response Variables (Cronbach α = .84)	RW	SRW	Err σ^2
W06...I check that virus protection software is enabled and updated.	1.00	0.62	1.35
W08...I check for new versions of virus protection software.	0.97	0.68	0.90
W09...I review virus protection software logs for scheduled updates and drive scans.	0.98	0.67	1.01
W16...I store email on my computer rather than the email server.	0.84	0.63	0.91

Table 26c

ISP@H item subscales. Lastly, the retained ISP@H measures were aggregated into access control (TA), physical protection (TP), security management (TS), user authentication (TU), and encryption (TE) item subscales. Respectively, Tables 27a, 27b, 27c, 27d, and 27e list the retained ISP@W measures and statistics for the corresponding item subscales.

ISP@H Access Control (TA) Item Subscales

Retained ISP@H Item-response Variables (Cronbach α = .71)	RW	SRW	Err σ^2
H10...personal firewall software monitors traffic into / out of my computer(s).	1.62	0.61	1.62
H11...as I surf the Web, I allow my Web browser to accept cookies from Web sites.	1.18	0.54	1.18
H13...I remotely connect to other computers and share drives, printers, or files.	0.97	0.52	0.97
H14...I use file transfer software to securely move files between computers.	1.33	0.65	1.33
H15...I store email on my computer rather than the email server.	1.07	0.51	1.07
H21...virus protection software has identified and limited virus impact to my computer.	1.19	.51	1.84

Table 27a

ISP@H Physical Protection (TP) Item Subscales

Retained ISP@H Item-response Variables	RW	SRW	Err σ^2
H04...I back-up my data to reliable media (disks, CDs).	1.08	.53	1.38

Table 27b

ISP@H Security Management (TS) Item Subscales

Retained ISP@H Item-response Variables (Cronbach α = .66)	RW	SRW	Err σ^2
H08...I check for new versions of virus protection software.	1.24	.55	1.64
H09...I review virus protection software logs for scheduled updates and drive scans.	1.20	.53	1.63
H28...I have other email account(s) forwarded to one main email account.	.90	.54	.91

Table 27c

ISP@H User Authentication (TU) Item Subscales

Retained ISP@H Item-response Variables (Cronbach α = .66)	RW	SRW	Err σ^2
H22...I routinely choose to change my password(s).	1.15	.63	.89
H25...I use a character sequence like Ij4Gf4Se%f# as my computer password.	1.02	.51	1.32

Table 27d

ISP@H Encryption (TE) Item Subscales

Retained ISP@H Item-response Variables (Cronbach α = .61)	RW	SRW	Err σ^2
H17...I encrypt confidential files with passwords.	1.18	.57	1.29
H18...I look for "https://" before I make financial transactions over the Internet.	1.33	0.54	1.33
H35...I use virtual private network (VPN) software to access other computers or other computer networks.	1.09	.55	1.23

Table 27e

Item subscales corroboration. Factor analysis (principle axis factoring extraction with equamax rotation) corroborated the item subscales *a priori* relevance. However, the numbers of factors derived were different based on use of the correlation matrix versus the covariance matrix. Factor analysis for eigenvalues over one was performed using both matrices. The results of both factor analyses also corroborated the content analysis results for RQ1.

Scree Plot of Item Subscales using the correlation matrix

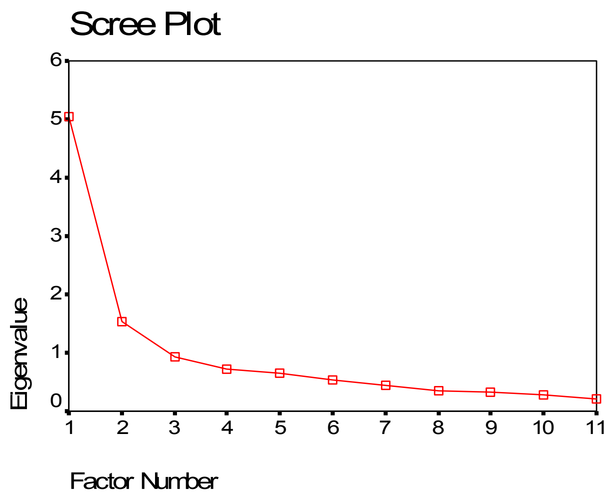


Figure 11

Item Subscales Factor Loadings using the correlation matrix

Item Subscales	Practice	Awareness
Technology (T)		.75
Policy (P)		.76
Threat-context (C)		.76
Deterrent (DE)	.57	
Preventive (PE)	.81	
Combined (DP)	.65	
Access Control (TA)	.68	
Physical Protection (TP)	.52	
User Authentication (TU)	.61	
Security Management (TS)	.61	
Encryption (TE)	.76	

Table 28

Using the correlation matrix, factor analysis identified awareness and practice as factors that explained 52% of item-response variance. Figure 11 depicts the scree plot where item subscales distinguished the two factors. Table 28 lists the factor loadings above .40.

Scree Plot of Item Subscales using the covariance matrix

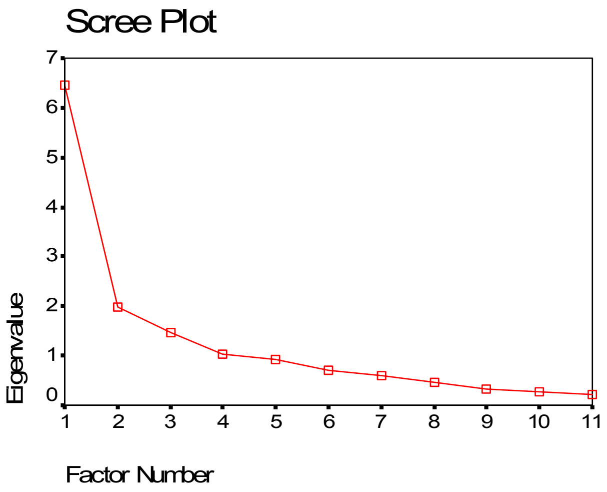


Figure 12

Items Subscales Loadings using the covariance matrix

Item Subscales	ISP@H	ISA	ISP@W
Technology (T)		.72	
Policy (P)		.78	
Threat-context (C)		.76	
Deterrent (DE)			.74
Preventive (PE) *	.53		.60
Combined (DP)			.59
Access Control (TA)	.77		
Physical Protection (TP)	.48		
User Authentication (TU)			.53
Security Management (TS)	.64		
Encryption (TE) *	.62		.43

*cross-loaded item subscales

Table 29

Using the covariance matrix, factor analysis identified three factors (ISA, ISP@W, and ISP@H) that explained 57% of response variance. Nine item subscales loaded evenly onto three factors and two item subscales loaded on both practice factors. Figure

12 depicts a scree plot of the factors that emerged. Also, Table 29 lists the factor loadings above .40.

The factor loadings, from Table 29, support the research model (refer to Figure 9 from Chapter II) that this study uses to compare information security trends between formal (ISP@W) and informal (ISP@H) environments. The three awareness subscales (T, P, and C) loaded solely onto the factor identified as ISA. Three formal practice subscales (DE, DP, and TU) loaded solely on ISP@W. Three informal practice subscales (TA, TP, and TS) loaded solely onto the factor identified as ISP@H. Therefore, comparisons and contrasts of these item subscales delineate commonalities and/or differences between factors. Also, the two cross-loaded item subscales provided similar practice distinctions between environments.

The cross-loadings (refer to Table 29) between item subscales PE and TE, as well as the loading of TU on ISP@W, were explained by practices within the context of a formal and/or informal computing-environment. Preventive and encryption practices were applicable to both formal and informal environments, so item subscales that represented these practices loaded on both formal and informal practice factors. However, user authentication practices were more applicable and originated within the formal computing-environment, so the TU item subscales loaded onto the formal practice factor.

Item subscales error variance estimates. From the initial CFA iteration, the factor variances for ISA, ISP@W, and ISP@H were estimated at .57, .82, and .45, respectively. SEM reliabilities ($\rho_{\text{subscales}}$) for each item subscales were available based on the squared sums of item regression weights applied to each factor variance, plus the sum of the individual item error variances. SEM item subscales unreliability ($1\text{-}\rho_{\text{subscales}}$) applied to the averaged items variance yielded the respective item subscales estimated error variance.

Table 30 lists the error variance estimates for the item subscales with multiple item-response variables. These nine error variances were held constant during in the CFA second iteration and the hybrid model analysis. By constraining or holding these particular item subscales error variances constant, individual item variances across the respective item subscales were maintained.

CFA and Hybrid Model Constant Subscales Error Variances

Item Subscales	var(Item$_{\text{Avg}}$)	∑ Reg. Wts.	∑ Var(Error)	Var(Error$_{\text{Subscales}}$)
Technology	1.07	4.22	4.83	0.34
Policy	1.55	3.27	5.57	0.74
Threat-context	0.90	10.62	8.68	0.11
Preventive	1.02	5.74	8.08	0.23
Combined	1.50	3.80	4.16	0.39
Access Control	0.94	7.49	9.11	0.25
User Authentication	1.25	3.33	4.18	0.57
Security Management	1.45	2.17	2.20	0.74
Encryption	1.27	3.45	4.36	0.56

Table 30

Retained ISA, ISP@W, and ISP@H Items

Based on the initial CFA iteration, an association and multiple regression (MR) analysis of retained ISA, ISP@W, and ISP@H measures identified awareness and/or practice relationships among the respective item-responses. Analysis of item-response variables, rather than item subscales, provided greater granularity for the second and fourth research questions. However, MR excludes measurement error estimation, so SEM (CFA and hybrid model analysis) was the superior statistical techniques for analysis of ISA domain measures based on item subscales. The between-construct associations and combined within/between relationships are reviewed later within the hybrid model results.

Appendix I lists the associations (r^2) or squared correlations (r) between retained ISA, ISP@W, or ISP@H item pairs. Effect sizes (Cohen, 1977) among the associations ($p<.05$) were categorized as large ($r^2 \geq .25$), medium ($r^2 < .25$ and $r^2 \geq .09$), and small ($r^2 < .09$). However, reduced power (<.90) limited distinguishing extremely small significant associations ($r^2 < .02$) or correlations ($r < .14$). The remainder of the analysis reviews within-construct associations and within-construct relationships.

Within-construct associations. Appendix I identified 279 unique within-construct associations ($p<.00$). One within-ISP@H pair (H25 and H15, where $r^2 = .01$ with $p<.02$) had reduced power (.49) and was not included as an association. Table 31 lists the frequencies, ranges, and average effects of unique within-construct associations.

Frequency and Range of Unique Within-Construct Associations

Construct	Large ($r^2 \geq .25$)	Medium ($.25 < r^2 \leq .09$)	Small ($r^2 < .09$)

ISA	n=27 (22%)
	Range .66 to .25
	Average = .30
		n=86 (72%)
		Range .24 to .09
		Average = .16
			n=7 (6%)
			Range .08 to .04
			Average = .06

ISP@W	n=7 (13%)
	Range .59 to .27
	Average = .41
		n=40 (73%)
		Range .21 to .09
		Average = .14
			n=8 (14%)
			Range .08 to .04
			Average = .07

ISP@H	n=6 (6%)
	Range .53 to .25
	Average = .34
		n=39 (37%)
		Range .24 to .09
		Average = .13
			n=59 (57%)
			Range .08 to .03
			Average = .06

Table 31

Summarizing the within-construct associations for ISA, ISP@W, and ISP@H item pairs; ISA pairs had more large effects, ISP@W pairs had more medium effects, and ISP@H pairs had more small effects. Therefore, ISA pairs explained large to medium amounts of awareness variance. ISP@W pairs explained mostly medium amounts of formal practice variance. Lastly, ISP@H pairs explained mostly small amounts of informal practice variance.

Among the respective within-construct, large-effect associations; four awareness items, two formal practice items, and four informal practice items were uniquely independent variables (UIVs). UIV variances were not explained by other large-effect, within-construct associations. Furthermore, UIV combinations within each respective construct explained ISA, ISP@W, and ISP@H item-response variances.

Table 32 identifies the survey item corresponding with each UIV. Awareness UIVs were among technology (A01), policy (A10), and threat-context (A11 and A14). Formal practice UIVs were deterrent-preventive (W09) and preventive (W14). Informal practice UIVs were among security management (H09), access control (H13), encryption (H17), and user authentication (H25).

Large-effect, Within-Construct UIVs

Construct	Uniquely Independent Item-response Variables
ISA	A01...that virus protection software can identify and remove known viruses. A10...that other users have suggested computer viruses can infect emails or email attachments. A11...that as a computer user, my knowledge of computer threats plays a significant role. A14...of the impact that a virus can have on my computer system.
ISP@W	W09...I review virus protection software logs for scheduled updates and drive scans. W14...I remotely connect to other computers and share drives, printers, or files.
ISP@H	H09...I review virus protection software logs for scheduled updates and drive scans. H13...I remotely connect to other computers and share drives, printers, or files. H17...I encrypt confidential files with passwords. H25...I use a character sequence like Ij4Gf4Se%f# as my computer password.

Table 32

Within-construct item relationships. Table 33 displays the results of ISA, ISP@W, and ISP@H items regressed over respective UIVs ($p<.05$). The resultant within-construct relationships explained item-response variances (adjusted R^2) over large or medium effect sizes, with no observed inverse relationships. Based on the highest SRW, MR also identified which UIV explained the most individual item-response variance. UIVs within the relationships were ordered by largest SRW strength and SRWs were omitted for table simplicity.

MR Explained Variance from Within-construct Relationships

ISA	R_{adj}^2	ISP@W	R_{adj}^2	ISP@H	R_{adj}^2
A01*+A10+A11+A14→**A02**	.72	W09*+W14→**W08**	.59	H09*→**H08**	.53
A14*+A11+A10+A01→**A13**	.55	W09*+W14→**W06**	.46	H13*+H17+H25→**H14**	.42
A14*+A10→**A15**	.49	W14*+W09→**W15**	.38	H09*+H13+H17→**H10**	.36
A14*+A10+A01+A11→**A19**	.42	W09*+W14→**W10**	.37	H25*+H17+H09→**H22**	.36
A11*+A10+A01→**A14**	.37	W09*+W14→**W04**	.22	H17*+H09+H25→**H04**	.23
A14*+A11+A10→**A16**	.35	W09*+W14→**W23**	.22	H17*+H09+H25→**H18**	.23
A14*+A11+A10→**A17**	.34	W09*+W14→**W16**	.19	H13*+H25+H17→**H35**	.23
A01*+A14+A11→**A10**	.32	W09*+W14→**W18**	.19	H13*+H25+H09→**H17**	.22
A10*+A11→**A09**	.31	W09*+W14→**W19**	.17	H13*+H17+H09→**H11**	.21
A11*+ A14+A01+A10→**A12**	.31	W14*→**W09**	.10	H17*+ H09→**H13**	.17
A01*+A10+A11→**A03**	.29	W09*→**W14**	.10	H09*+H25→**H21**	.17
A10*+A14+A11→**A01**	.28			H13*+H25+H09→**H28**	.16
A14*+A10+A01→**A11**	.28			H17*+H09→**H25**	.12
A10*+A14+A11→**A18**	.25			H25*+H17+H13→**H09**	.11
A10*+A01+A11→**A06**	.22			H17*+H13+H09→**H15**	.09
A10*+A01+A11→**A04**	.14				

* UIV with the stronger within-construct SRW.

Table 33

Within the awareness construct, 87% of the explained variances had large effect sizes. UIVs explained from 72% to 14% of each ISA measure. The technology domain (A01) explained the most ISA variance among 19% of the relationships. The policy domain (A10) explained the most variance among 31% of the relationships. Lastly, threat-context (A11 and A14) explained the most awareness variance among 50% of the relationships. On average, 35% of each awareness measure was explained by UIVs.

Therefore, ISA items were explained by large-effects where, over the majority of within-ISA relationships, threat-context awareness contributed the greatest explanation.

Among formal practice, 36% of the explained variances had large effect sizes. On average, 27% of each formal practice had UIV explanations. UIVs explained from 59% to 10% of each ISP@W practice. Also, the combined deterrent-preventive (W09) and the preventive (W14) ISA domain measures provided variance explanations among the formal practices. Therefore, preventive and deterrent-preventive efforts were stronger than deterrent efforts as explanations for formal practices. Furthermore, neither deterrent nor preventive efforts alone were sufficient explanations for formal practice variances, which concurred with Straub (1990) and Kankanhalli et al. (2003).

Informal UIVs explained from 53% to 9% of each informal practice, where 27% of all variances were large effects. Also, informal UIVs explained an average 24% of each ISP@H practice variance. Furthermore, stronger informal practice measures among UIVs were identified as access control (H13) and encryption (H17), which were stronger explanations among 67% of informal measures. The security management (H09) domain was the stronger UIV among 20% of the informal measures. Lastly, the user authentication (H25) domain was the stronger UIV among 13% of the informal measures. Therefore, H13 and H17, which represented ISA domain measures for access control and encryption, were stronger explanative UIVs among informal practices.

CFA Parameter Estimates

The second CFA iteration employed ISA, ISP@W, and ISP@H item subscales, along with the retained item-measures for PI and CSE. Appendix H depicted the second iteration CFA model and the corresponding estimated parameters. Unconstrained error terms and correlated error terms were omitted from Appendix H for figure simplicity. The CFA estimated parameter review follows for construct variances and correlations, within-construct relationships, and error term variances and correlations.

Construct variances and correlations. Based on the previously noted goodness-of-fit statistics, the second CFA iteration provided an adequate fit between the CFA model and the survey item-responses. All trait, awareness, and practice constructs were estimated with positive variances (p<.00) and positive correlations (p<.00). The construct correlation estimates ranged from .37 (ISP@W↔CSE) to .79 (ISP@W↔ISP@H). Also, the estimated correlation between PI and CSE was positively correlated (.61), which supported similar results from Thatcher and Perrewé (2002).

Within-construct relationships. Strong, large-effect relationships were estimated within each CFA construct. Each item-response or item subscales measure yielded a SRW estimate greater than .50 (p<.00), with SMC estimates ranging from .32 to .88. Table 34 identified the strongest, within-construct relationships from Appendix H.

Relationship results from the second CFA iteration also supported the association and MR analysis of individual within-awareness and within-practice item-responses. However, association and MR analysis of individual within-practice item-responses also identified other strong within-practice explanations from formal deterrent-preventive efforts (W09) and informal security management (H09) ISA domain measures. The CFA results (refer to Appendix H) acknowledged these stronger within-practice explanations, but also accounted for the higher error variance among these practice measures, which resulted in weaker relationships (SRWs) when compared to preventive efforts and access control measures. CFA results controlled for error when corroborating the MR analysis.

CFA Estimates for Item or Item Subscales Largest Explanations			
Construct	Item or Item Subscales	SRW	SMC
CSE	CSE04…if I had seen someone else using it before trying it myself?	.87	.77
ISP@W	Preventive efforts practice	.88	.77
ISA	Threat-context awareness measures	.94	.88
PI	PI03…I seek out new ways to do things.	.83	.70
ISP@H	Access control practices	.85	.67

Table 34

Error term variances and correlations. The SEM literature noted that error term correlation provided a means to compensate for systematic error within the measurement instrument. Error term correlations reflected independent error terms that measured commonalities among error measurements, which were not represented in the CFA model (Kline, 1998). However, Appendix H omitted the unconstrained, exogenous error term variances for deterrent efforts, physical protection, and individual user trait measures (CSE and PI), along with all error term correlations. Table 35 lists the omitted estimated error term variances (p<.00).

Individually, error terms were exogenous, one-dimensional, and independent measures. However, correlation between individual error terms yielded unknown commonalities, which were not present as part of the CFA model. Tables 36a and 36b list correlated error terms between constructs and the estimated correlations among ISA-to-ISP@W and ISP@W-to-ISP@H measures, respectively. Also, Tables 36c, 36d, and 36e list correlated error terms from within constructs and the estimated correlations among respective individual awareness, formal practice, and informal practice measures.

Tables 36f and 36g list correlated error terms within trait constructs and the estimated correlations among CSE and PI measures, respectively.

CFA Estimated Error Variances for Item-Subscales and Individual Traits

Item-response	Estimated Error σ^2	Item-response	Estimated Error σ^2
Deterrent Efforts	1.01		
Physical Protection	1.43	PI01	.66
CSE01	.62	PI02	.37
CSE02	.68	PI03	.36
CSE03	.44	PI05	.50
CSE04	.29	PI08	.62
CSE05	.25	PI09	.50
CSE06	.34	PI11	.47
CSE07	.33	PI12	.64
CSE08	.44	PI14	.46
CSE09	.34	PI18	.43
CSE10	.39	PI19	.54

Table 35

CFA ISA-to-ISP@H Correlated Error Terms (p<.00)

Correlated Error Terms	Estimated Correlation
technology awareness ↔ access control	**+0.25**
technology awareness ↔ security management	+0.22

Table 36a

ISP@W-to-ISP@H Correlated Error Terms (p<.00)

Correlated Error Terms	Estimated Correlation
deterrent efforts ↔ user authentication	+0.35
preventive efforts ↔ encryption	**+0.54**
deterrent-preventive efforts ↔ physical protection	-0.18
deterrent-preventive efforts ↔ access control	**-0.41**

Table 36b

From correlated error terms between constructs (refer to Tables 36a and 36b), several ISA domain commonalities were observed. Individual technology awareness was common with informal practice of access control and security management. Likewise, formal deterrent efforts were common with informal user authentication practice. Formal preventive efforts were also common with informal encryption practice. However, formal deterrent-preventive efforts had common differences among informal physical protection and access control practice.

CFA Within-ISA Correlated Error Terms (p<.00)	
Correlated Error Terms	Estimated Correlation
technology awareness ↔ threat-context awareness	**-0.79**

Table 36c

CFA Within-ISP@W Correlated Error Terms (p<.02)	
Correlated Error Terms	Estimated Correlation
preventive efforts ↔ deterrent-preventive efforts	**-0.16**

Table 36d

CFA Within-ISP@H Correlated Error Terms (p<.00)	
Correlated Error Terms	Estimated Correlation
access control ↔ user authentication	**-0.20**
access control ↔ security management	**+0.14**

Table 36e

The correlated error terms within individual awareness, formal practice, and informal practice constructs (refer to Tables 36c, 36d, and 36e, respectively) also revealed commonalities and differences between ISA domain measures. Informal practice across the ISA domain measures of access control and security management had commonality between measurement error terms. However, individual technology versus threat-context awareness, formal preventive efforts versus deterrent-preventive efforts practice, and informal access control versus user authentication practice had common differences. Among all within-construct and between-construct correlated measurement errors, the individual ISA domain measures of technology and threat-context awareness had the strongest common difference. Therefore, high measurement error in one ISA domain measure corresponded with low measurement error in the other.

Within-CSE Correlated Error Terms (p<.00)

Correlated Error Terms	Estimated Correlation
CSE01 ↔ CSE02	**+0.74**
CSE01 ↔ CSE03	+0.34
CSE01 ↔ CSE09	-0.24
CSE02 ↔ CSE03	+0.34
CSE02 ↔ CSE09	-0.24
CSE04 ↔ CSE07	-0.26
CSE04 ↔ CSE08	**-0.32**
CSE05 ↔ CSE08	-0.28
CSE05 ↔ CSE06	+0.27
CSE06 ↔ CSE07	+0.22
CSE06 ↔ CSE09	+0.30
CSE09 ↔ CSE10	+0.42

Table 36f

Within-PI Correlated Error Terms (p<.00)

Correlated Error Terms	Estimated Correlation
PI01 ↔ PI08	+0.14
PI01 ↔ PI02	+0.24
PI02 ↔ PI03	**+0.47**
PI08 ↔ PI09	+0.25
PI08 ↔ PI12	+0.20
PI09 ↔ PI14	+0.27
PI11 ↔ PI12	+0.26
PI11 ↔ PI14	+0.25
PI11 ↔ PI18	**-0.19**
PI12 ↔ PI14	+0.24
PI18 ↔ PI19	+0.18

Table 36g

RQ1, RQ2, RQ3, and RQ4 CFA Supported Answers

Answers to the second, third, and fourth research questions, posed from Chapter II, were provided within the CFA results. Furthermore, the CFA results also supported the content analysis answer to the first research question. This section reviews each research question answer, along with the supporting CFA results.

What is the domain of information security awareness (RQ1)? The content analysis results identified the characteristics of the user-level ISA concept as ISA domain measures among individual users and computing-environments. The first iteration CFA identified ISA domain measures with stronger relationships (SRW/SMC). Factor analysis of the aggregated domain measures (item subscales) substantiated the differences and similarities among the ISA domain measures (ISA characteristics).

During the second iteration CFA, all identified ISA domain measures were retained with strong large-effects (refer to Appendix H). Threat-context was the strongest ISA domain explanation and the stronger individual ISA relationship, while technology was a stronger individual ISA relationship beyond policy. Also, formal and informal ISA domain measures yielded similar stronger relationships among work and home computing-environments, respectively. Among the formal ISA domain measures, preventive efforts were the strongest explanation and deterrent-preventive efforts were stronger than deterrent efforts. Access control was the strongest explanation among informal ISA domain measures, followed by encryption, security management, user authentication, and physical protection. Therefore, the CFA results supported the content analysis answer to research question RQ1.

What are measures of information security awareness (RQ2)? PI was the only trait construct that had scale measures (late majority and laggards) rejected during the first CFA iteration for lack of relationship (p>.05). Moreover, the CSE and PI constructs yielded positive estimated correlations (p<.00) between individual ISA, ISP@W, and

ISP@H. Also, the ISP@W and ISP@H constructs yielded positive estimated correlations (p<.00) with individual ISA from the second iteration CFA (refer to Appendix H). Therefore, each construct retained measures that correlated and were associated with individual ISA. Furthermore, the correlations (p<.00) estimated by the 2nd iteration CFA supported ISA domain measures (item subscales) as measures of individual ISA. Hence, high or low measures within a particular construct (PI, CSE, ISP@W, or ISP@H) corresponded to proportional high or low individual ISA measures.

Within the individual ISA construct, policy awareness measures were dropped because of weak relationships that were due to lack of respondent understanding or other ISA measures with stronger relationships. Also, policy awareness was the weaker explanation of the three individual ISA measures. Thus, policy represented weaker ISA measures than technology awareness and both represented weaker ISA measures when compared to threat-context knowledge. Moreover, correlated measurement error between technology and threat-context awareness measures indicated that strong commonality was inversely related as a common difference. High threat-context awareness offsets low technology awareness, while high technology awareness offsets low threat-context awareness.

Among the threat-context ISA measures, awareness that individual knowledge of computer threats plays a significant role (A11) and awareness of the impact that a virus can have on a computer system (A14) were stronger explanations. However, between-construct ISA measures also provided explanations, as evidenced by the error term correlations between individual technology awareness and informal access control or security management practices. Therefore, SEM hybrid model results of between-construct relationships provided further granularity for answering research question RQ2.

Which information security practices reflect individual ISA (RQ3)? Within the formal environment, decision-makers used threat-context awareness to develop formal or informal security policy. Policy awareness, manifested within deterrent efforts practice, was the weakest formal explanation. Technology awareness grounded within security policies, manifested as deterrent-preventive efforts practice, was stronger than the deterrent efforts explanation. However, technology awareness outside of security policy, manifested within preventive efforts practice, provided the strongest formal explanation.

Within the informal environment, the individual user was the decision-maker, who used various measures of threat-context awareness for individual informal security practice. The informal practice measures, ordered by strength of explanation, were access control, encryption, security management, user authentication, and physical protection. Among these informal practice ISA domain measures, the top three ISP@H practice measures were associated with security threat countermeasures (threat-context awareness) beyond the physical boundaries of the home computing-environment.

From retained formal and informal practice, both ISP@W ($\rho \approx .43$) and ISP@H ($\rho \approx .48$) yielded positive ISA correlation estimates ($p<.00$). Accordingly, high or low measures within ISP@W or ISP@H corresponded with proportional high or low ISA measures. However, informal practice had the higher estimated correlation. Therefore, SEM hybrid model results provided further granularity in answering research question RQ3.

Do security practices differ between computing-environments (RQ4)? The second CFA iteration estimated high positive correlation ($\rho \approx .79$ at $p<.00$) between ISP@W and ISP@H constructs. Accordingly, retained formal practice had high or low measures that corresponded with proportionally high or low informal practice. Also, many of the security practice measures surveyed between environments were identical. Hence, high positive correlation between practice measures in different environments should indicate few differences. However, the different computing-environments yielded noted inconsistencies among dropped and retained CFA practice measures.

Similar retained and dropped practice measures within both computing-environments had observed and unobserved differences. Many of the weak (SRW < .5) formal and informal measures, dropped during the first CFA iteration, were noted to differ, yet were not reflected in the second CFA iteration. Furthermore, the awareness that generated practice decisions within each environment had different unobserved origins. Dropped items differed when practice decisions were made by the individual user (informal) rather than an individual user adhering to security policy (formal). Hence, policy contradictions were irrelevant and risky practice was more convenient in the absence of security policy. Informal technology awareness also differed, since the majority of respondents relied less on university supplied virus protection software. Also, correlated error terms between deterrent-preventive efforts and informal physical protection or access control practice had common differences outside of the CFA model. Therefore, the hybrid model results and known-groups results provided further granularity in answering research question RQ4.

Results of Hybrid Model Analysis

The SEM hybrid model was similar to the CFA model. However, the research model's hypothesized relationships among ISA, ISP@W, ISP@H, PI, and CSE (the user-level ISA concept) replaced CFA construct correlations, which increased between construct analyses granularity. Exogenous disturbance terms were added to each awareness and practice construct, which accounted for unexplained ISA, ISP@W, and ISP@H variances outside of the user-level ISA concept explanation. The SEM hybrid model goodness-of-fit statistics gave credibility to within and between construct reviews of retained individual traits, awareness, and practice. Hypothesized construct relationships or paths, as well as ISA domain measures within each respective construct, provided answers to the second, third, fourth, fifth and sixth research questions. Also, the path relationships answered research hypotheses H1, H2, H3, H4, and H5. Appendix J depicts the hypothesized user-level ISA concept as a SEM hybrid model. As with the CFA model (refer to Appendix H), unconstrained hybrid model error terms and correlated error terms were omitted for model readability and simplicity.

SEM hybrid model analysis results yielded estimated parameters for hypothesized path relationships between constructs, standardized effects between constructs, explained and unexplained variances among the awareness and practice constructs, along with error term variances and correlations. Also, association and MR analysis between awareness and practice measures provided additional ISA domain measure granularity. Detailed discussion of these results follows after a review of the hybrid model goodness-of-fit statistics. The section concludes with the supported answers to research questions RQ2, RQ3, RQ4, RQ5, and RQ6.

SEM Hybrid Model Fit

Appendix J depicts the SEM hybrid model where exogenous variables PI, CSE, disturbance terms, and unconstrained SEM error terms represented hypothesized relationships. ISA, ISP@W, and ISP@H constructs were converted to endogenous variables with the inclusion of exogenous disturbance terms for each construct (d1, d2, and d3, respectively). The endogenous constructs along with observed item-responses and constrained error terms also explained the respective relationships among the exogenous variables. The recursive and identified hybrid model was an adequate, representative fit for the 531 item-responses, as indicated by the supporting goodness-of-fit statistics: CMIN/DF, GFI, CFI, RMR, SRMR, and RMSEA. These selected indices were identified during earlier CFA model fit discussions and Table 37 lists the hybrid model goodness-of-fit statistics along with the second iteration CFA model fit statistics for model comparisons. Also, comparing parameter estimates between Appendix H (SEM CFA model) and Appendix J (SEM hybrid model) provided an additional check of the hybrid model fit.

Comparison of SEM Hybrid vs. CFA Model Goodness-of-Fit Statistics

Model	CMIN / DF			GFI	CFI	RMR	SRMR	RMSEA		
	X^2	DF	Ratio					Value	90% C.I.	H_0 p-value
Hybrid	987.9	432	2.29	.90	.96	.07	.06	.049	.045 Lo .053 Hi	.61
CFA	972.7	430	2.26	.90	.96	.07	.06	.049	.045 Lo .053 Hi	.68

Table 37

Table 37 illustrates the few differences found when comparing goodness-of-fit statistics between the SEM models. The X^2 statistic, model degrees of freedom, and CMIN/DF ratio increased slightly with the introduction of path relationships and disturbance terms, yet the CMIN/DF ratio remained below the cut-off of 3.0. The RMSEA p-value for the H_0 closeness of fit test decreased. However, the RMSEA p-value remained greater than .5, which supported the hypothesis that the RMSEA was "good" in the population. The remaining goodness-of-fit statistics remained unchanged.

Also, comparing common estimated parameters between Appendix H and Appendix J found few differences, which were all associated with the PI construct. The PI construct had slight decreases of .01 in the estimated correlation with CSE and in the estimated PI variance. Also, the strength of estimated PI construct SRWs had slight increases and decreases. Item-response variable PI19 had an increase of .02. Item-response variables of PI18, PI12, and PI09 had increases of .01. Lastly, item-response variables PI05 and PI02 had decreases of .01. Therefore, the strength of within-construct SRWs experienced little to no change between the CFA and hybrid models when between-construct path relationships replaced construct correlations.

Hypothesized Path Relationships H1, H2, H3, H4, and H5

From Chapter II, construct relationships were hypothesized within the user-level ISA concept. The SEM hybrid model (refer to Appendix J) quantified and retained all hypothesized relationships ($p<.00$). Table 38 details each of the between-construct, direct relationships from the research model. The power (Cohen, 1977) of each hypothesis test was estimated at 1.00, with the sample size of 531 and a significance level of $\alpha = .05$.

User-level ISA Concept Direct Relationships (p<.00)

Relationship	Retained Hypothesis	SRW
ISA→ISP@W	H1: Higher measures of user-level ISA should positively affect user information security practices at work.	.77
ISA→ISP@H	H2: Higher measures of user-level ISA should positively affect user information security practices at home.	.33
ISP@W→ISP@H	H3: Information security practices at work, which have high measures of user-level ISA perspectives of policy and technology, should positively affect user information security practices at home.	.79
PI→ISA	H4: High measures of user-level PI should positively affect high measures of ISA.	.30
CSE→ISA	H5: High measures of user-level CSE should positively affect high measures of ISA.	.29

Table 38

From Table 38, both PI and CSE explained individual ISA. Individual ISA had the stronger direct relationship when explaining formal practice over informal practice. Also, formal practice had the stronger direct explanation of informal practice variance. Accordingly, PI and CSE had effects on both ISP@W and ISP@H through the path relationships with ISA. Therefore, ISA mediated the relationships between PI and CSE over ISP@W and ISP@H. Furthermore, ISP@W also partially mediated the effects of PI, CSE, and ISA over ISP@H. Details of each construct's influence on ISP@H are discussed later under standardized direct and indirect effects.

Association and MR Analysis

Based on CFA model results, an association and multiple regression (MR) analysis of retained ISA, ISP@W, and ISP@H measures identified awareness and/or practice relationships among the respective item-responses. Analysis of item-response variables, rather than item subscales, provided greater ISA domain granularity for the second, third, and fourth research questions. However, the fact that MR excludes measurement error estimation was noted earlier, so SEM was the superior statistical technique for ISA domain analysis.

Appendix I listed the associations (r^2) between retained ISA, ISP@W, or ISP@H item pairs. As with previously noted CFA results, association effect sizes were also categorized and limited due to power (<.90). Reviews of between ISA and practice associations; between ISA and practice relationships; between practice associations and relationships; and combined ISA and/or practice relationships follow.

<u>Between ISA and practice associations</u>. From Appendix I, 73% of the ISA-to-practice measure pairings were associations ($p<.05$). However, none of the associations yielded large effects. Table 39 summarizes the frequencies, ranges, and effect averages of ISA-to-practice associations from Appendix I.

ISA-to-practice associations identified formal and informal practice that reflected awareness measures. From Table 39, the majority of awareness associations were small for both environments. However, eight informal practice measures (H08, H09, H10, H11, H14, H18, H21 and H35) had medium-effect awareness associations, which out-numbered the four formal practice measures (W06, W08, W09, and W10) with medium-effect associations.

Frequency and Range of ISA-to-practice Associations

Between Constructs	Medium $(.25 > r^2 \geq .09)$	Small $(.09 > r^2 \geq .02)$	None $(.02 > r^2 \geq .00)$

ISA-to-ISP@W	n=13 (7%)
	Range .13 to .09
	Average = .10
		n=118 (68%)
		Range .08 to .02
		Average = .04
			n=27 (15%) ($p>.05$)
			n=18 (10%) ($r^2=.01$, $p<.05$)

ISA-to-ISP@H	n=18 (7%)
	Range .19 to .09
	Average = .11
		n=155 (65%)
		Range .08 to .02
		Average = .04
			n=37 (15%) ($p>.05$)
			n=30 (13%) ($r^2=.01$, $p<.05$)

Table 39

Conversely, consistent lack of association identified practice measures that did not reflect awareness measures. Appendix I noted that lack of awareness association (27%) was present among formal (25%) and informal (28%) practice. Four UIVs (A01-69%, A10-50%, A14-62%, and H13-88%) had consistent high lack of association among ISA-to-practice pairings. Also, technology awareness item A02 (65%), threat-context awareness item A13 (46%), preventive efforts practice W04 (44%), access control practice H15 (63%), and security management practice H28 (69%) were consistently high among lack of awareness association pairings. Therefore, awareness measures A01, A02, A10, A13, and A14 were consistent in lack of ISA-to-practice associations. Furthermore, informal practice reflected fewer awareness measures than formal practice. In particularly, informal practice H13 reflected the least number of awareness associations over the informal practice ISA domain measures for access control.

Between ISA and practice relationships. MR yielded ISA-to-practice relationships that explained similar medium to small effect sizes (adjusted R^2) as associations from Appendix I. However, MR distinguished the stronger awareness explanations for formal and informal practice and/or UIVs. Furthermore, review of the ISA-to-practice relationships showed that awareness measures were not consistent across the ISP@W and ISP@H constructs. Table 40 details the MR results ($p<.05$) of practice measures over awareness measures, ordered by SRW strength. Also, SRWs were omitted for table simplicity.

MR ISA-to-practice Relationships by Effect Size

ISP@W Relationships	R_{adj}^2	**ISP@H Relationships**	R_{adj}^2
A03*+A18+A19-A02+A06+A17 →**W06**	**.20**	**A04***-A06+A15 -A13+A02+A17+A19+A11+A03→**H08**	**.24**
A04*-A01+A18+A03+A19+A09→**W10**	**.19**	**A04***+A17-A06-A13+A03+A19+A09→**H10**	**.24**
A17*+A18+A03-A14+A06 →**W08**	**.16**	**A04***+A15-A06+A17+A09-A13→**H09**	**.18**
A18*+A12-A14+A04→**W15**	**.12**	**A15***+A11+A01-A13-A12+A19+A18→**H21**	**.17**
A18*+A06+A09-A13→**W09**	**.12**	**A04***+A18+A17-A14-A02→**H35**	**.17**
A18*+A16+A15-A14→**W18**	**.12**	**-A14***+A15+A16+A12+A09+A04→**H18**	**.16**
A16*+A12+A04-A14→**W19**	**.12**	**A09***-A10+A19-A02+A11+A03+A16→**H25**	**.15**
A13*-A14+A04-A02+A16+A06→**W14**	**.09**	**A04***+A18→**H11**	**.13**
A18*+A12→**W04**	**.08**	**A18***+A04+A15-A14→**H14**	**.12**
A19*+A04-A02→**W23**	**.08**	**A18***-A02+A09+A17+A04→**H17**	**.12**
-A02*+A18+A12+A09→**W16**	**.07**	**A19***+A04+A09-A02-A06+A11→**H22**	**.12**
		A12*+A19+A03-A06→**H04**	**.09**
		A04*+A18→**H28**	**.05**
		-A14*+A16+A18+A15→**H15**	**.04**
		A04*→**H13**	**.03**

* Stronger ISA-to-practice SRW

Table 40

ISA-to-ISP@W relationships. The ISA-to-ISP@W relationships from Table 40 explained from 20% to 7% of each formal practice variance. On average, awareness measures explained 12% of a formal practice. Therefore, awareness had a medium effect on explaining ISP@W. However, two awareness UIVs (A10—policy and A11—threat-context) were not identified within the ISA-to-ISP@W relationships. Hence, awareness measures A10 and A11 were not reflected among formal practice explanations.

Four other awareness items (A01—UIV technology, A02—technology, A13—threat-context, and A14—UIV threat-context) had inverse relationships when explaining formal practice. Both awareness UIVs and item A02 maintained inverse relationships among all the applicable formal practice explanations. The strongest inverse relationship observed was between technology awareness item A02 and the deterrent-preventive effort W16. Also, the threat-context awareness item A13 had one inverse relationship with deterrent-preventive effort W09. Therefore, awareness measures with consistent lack of ISA-to-ISP@W association had inverse relationships among formal practices (with the exception of W04).

Summarizing all ISA-to-ISP@W relationships from Table 40, threat-context awareness was stronger among 81% of the formal practices. Technology awareness was stronger among the remaining formal practices (19%). Policy awareness was present among 55% of the formal practice explanations, yet policy awareness was never identified as a stronger awareness measure. Therefore, threat-context and technology awareness measures had stronger explanations of formal practice variance. In particularly, threat-context awareness item A18 was the stronger explanation among 36% of the formal practice measures.

ISA-to-ISP@H relationships. From Table 40, all awareness items were identified among formal practice explanations. Awareness explained from 24% to 3% of individual informal practice variance. On average, awareness explained 13% of an informal practice. Therefore, awareness had a medium effect on explaining informal practice variance. Furthermore, all awareness items directly contributed as strong awareness explanations to particular ISP@H practice variances.

Six awareness items (A02—technology, A06—policy, A10—UIV policy, A12—threat-context, A13—threat-context, and A14—UIV threat-context) had inverse relationships when explaining 73% of the informal practice measures. The awareness UIVs, A02, A06, and A13 maintained inverse relationships among all the respective ISP@H practice explanations. The strongest inverse relationship observed was between awareness UIV item A14 and the encryption practice H18. The threat-context awareness item A12 yielded one inverse relationship with access control practice H21. Therefore, awareness measures with consistent lack of ISA-to-ISP@H association had inverse relationships among informal practice (with the exceptions of H04, H11, H13, and H28). Furthermore, awareness items A06 and A12 had low ISA-to-ISP@H association (.03 on average), which also resulted in inverse relationships among particular informal practice measures.

Summarizing all the informal practice explanations from Table 40, threat-context (46.6%) and technology (46.6%) awareness measures were stronger among 93% of the informal practice measures. Both technology and threat-context awareness measures were present in all informal practice explanations. Policy awareness was also present among explanations in 53% of informal practice. Unlike ISP@W, policy awareness (A09) was stronger among the explanations for user authentication UIV (H25). Also, technology awareness item A04 was stronger among explanations for seven ISP@H practice measures: three access control (H10, H11, and H13), three security management (H08, H09, and H28), and one encryption (H35). Therefore, all awareness measures were strong explanations of informal practice variance. In particularly, technology awareness item A04 was the strongest explanation among 47% of informal practice variances.

Between practice associations. From Appendix I, 96% of ISP@W-to-ISP@H (formal-to-informal) pairings were associations ($p<.05$). Unlike ISA-to-practice pairs, formal-to-informal practice pairs yielded large effect associations (r^2). Seven pairings (W04/H04, W10/H10, W15/H14, W16/H15, W18/H17, W19/H18, and W23/H22) were common measures between environments that yielded large effect associations. Three pairings (W08/H08, W09/H09, and W14/H13) were common measures between environments that yielded medium effect associations. Moreover, two of the medium-effect common measures were also formal (W09 and W14) and informal (H09/H13) UIVs. However, the majority of association effects were small. Table 41 lists the frequencies, ranges, and effect averages of ISP@W-to-ISP@H pairings.

Frequency and Range of ISP@W-to-ISP@H Associations by Effect Size

Large ($r^2 \geq .25$)	Medium ($.25 > r^2 \geq .09$)	Small ($.09 > r^2 \geq .02$)	None ($.02 > r^2 \geq .00$)

n=8 (5%)
Range .60 to .25
Average = .26
	n=43 (26%)
	Range .19 to .09
	Average = .13
		n=108 (66%)
		Range .08 to .02
		Average = .05
			n=2 (1%) ($p>.05$)
			n=4 (2%) ($r^2=.01$, $p<.05$)

Table 41

Between practice relationships. MR of informal measures over formal practice measures yielded relationships ($p<.05$) with larger effect sizes (adjusted R^2). Also, MR distinguished formal explanations for informal practice measures and UIVs. Table 42 detailed these results ($p<.05$), ordered by the stronger formal practice SRWs that were omitted for table simplicity.

From Table 42, all formal practice measures directly contributed ($p<.05$) to particular ISP@H variance explanations. Formal practice measures explained from 61% to 13% of individual informal practice variance. On average, formal measures explained 29% of an informal practice. Also, excluding the deterrent-preventive effort W06, each formal practice was a stronger explanation for a particular informal practice. Therefore, formal practice measures yielded an average large-effect explanation of informal practice variance.

MR Formal-to-Informal Practice Relationships by Effect Size

ISP@W-to-ISP@H Relationships	R_{adj}^2
W19*+W04→H18	.61
W15*+W10-W08+W19→H14	.47
W18*+W15→H17	.41
W23*+W18+W10-W14→H22	.40
W10*-W08+W06+W19+W18+W23→H10	.31
W15*+W08+W14+W10+W18→H35	.31
W04*+W19+W18-W16+W09→H04	.29
W08*+W19+W10-W15+W18→H08	.27
W16*→H15	.26
W09*-W08+W19+W10+W18-W15→H09	.24
W14*+W15+W18→H13	.19
W23*+W10+W18+W16→H25	.17
W10*+W15+W16+W19-W06→H28	.16
W14*+W19+W15+W16→H11	.13
W10*-W08+W06+W19+W18+W23-W15→H21	.13

* Stronger ISP@W-to-ISP@H between construct SRW

Table 42

Formal practice ISA domain measures of deterrent efforts, preventive efforts, and combined deterrent-preventive efforts were stronger explanations for particular informal practice measures. Deterrent effort (W23) was present among explanations in 27% of the informal measures. However, deterrent effort W23 was stronger among explanations for the informal practice of user authentication, which categorized informal measures H22 (40%) and H25 (17%). Item-responses W23 and H22 were common measures between the formal and informal environments. Also, informal practice H25 was an UIV. Therefore, within the user authentication measures, deterrent effort W23 explained an average large-effect of 29% for each informal practice.

Preventive efforts were present among explanations in 93% of the informal measures. Preventive efforts (W04, W10, W14, W15, W18, and W19) were stronger explanations among common informal practice within four distinct ISA domain measures: physical protection (W04/H04), access control (W10/H10, W14/H11, W14/H13, W15/H14, and W10/H21), encryption (W18/H17, W19/H18, and W15/H35) and security management (W10/H28). Six common formal and informal measures (W04/H04, W10/H10, W14/H13, W15/H14, W18/H17, and W19/H18) were preventive effort explanations that explained an average 38% of the common informal practice. Also, informal measures H13 and H17 were UIVs that were explained by the respective, common formal practice W14 or W18. Therefore, preventive effort large-effect explanations were most frequent among informal practice. Furthermore, the access control measures had more large-effect preventive efforts explanation.

Combined deterrent-preventive efforts were present among explanations in 67% of the informal measures. Deterrent-preventive efforts were stronger among explanations for three common measures between environments over two informal ISA domain measures: access control (W16/H15) and security management (W08/H08 and W09/H09). Deterrent-preventive efforts explained an average 26% of these informal measures. Also, the common practice (W09/H09) was both a formal and informal UIV. Therefore, deterrent-preventive efforts were an average, large-effect explanation for informal practice within the ISA domain measures of access control and security management.

Five formal measures (W15—preventive effort; W06, W08, and W16—combined deterrent-preventive efforts; and W14—UIV preventive effort) had inverse relationships when explaining 53% of the informal measures. However, the inverse relationships were not maintained nor were inverse relationships the strongest SRW among the formal explanations. Therefore, informal practice (excluding H11, H13, H15, H17, H18, H25, and H35) yielded inverse relationships among particular preventive and deterrent-preventive formal practice measures.

Summarizing all the ISPW-to-ISP@H relationships from Table 42, deterrent efforts (13%), preventive efforts (67%), and deterrent-preventive efforts (20%) were stronger explanations among particular informal measures. However, each formal practice ISA domain measure was not inclusive to all informal measures. Therefore, preventive efforts as a formal practice were a stronger explanation of informal practice variance. In particularly, preventive effort W19 was the strongest explanation for informal practice H18. Also, preventive effort W10 was included among 60% of the informal measures.

Combined between ISA and/or practice relationships. As previously noted in Chapter II, Stanton et al. (2005) found that small increases in security awareness (ISA-to-practice relationships) shifted improvement in security behavior (ISP@W and ISP@H practice). Furthermore, Leach (2003) stated that increased security practice (ISA-to-practice and ISP@W-to-ISP@H relationships) strengthen security behavior. Hence, medium to small effects from ISA-to-practice relationships yielded medium to large effect relationships when formal and informal practice UIVs were included. Likewise, medium to large effects from ISP@W-to-ISP@H relationships were strengthened when informal practice UIVs were included.

MR Combined Awareness and Practice Relationships by Effect Size			
ISP@W Relationships	R_{adj}^2	**ISP@H Relationships**	R_{adj}^2
__W09*__+__A17*__+W14→__W08__	.61	__H09*__+__A02*__+A19+A03+A10 →__H08__	.58
__W09*__+__A19*__+A03+A17+ W14→__W06__	.51	__H13*__+H17+__A04*__+H25→__H14__	.44
__W09*__+__A15*__+A18→__W10__	.39	__H09*__+__A04*__+H13+A03→__H10__	.42
__W14*__+W09+__A18*__→__W15__	.39	__H25*__+H17 +H09 +__A19*__→__H22__	.37
__W09*__+W14+__A18*__→__W04__	.24	__H13*__+H25+__A04*__+H17→__H35__	.27
__W09*__+W14+__A19*__→__W23__	.24	__H17*__+__A16*__+H09+H25→__H18__	.26
__W09*__+W14+__A18*__→__W18__	.21	__H17*__+ H09+__A12*__+H25→__H04__	.25
__W09*__+W14+__A04*__+A11→__W19__	.20	__H13*__+__A04*__+H17→__H11__	.25
__W14*__+__A18*__+A04→__W09__	.16	__H13*__+__A18*__+H25+H09→__H17__	.24
__W09*__+__A04*__→__W14__	.12	__H09*__+__A01*__+A15+A11+H25→__H21__	.24
__W14*__+__A18*__→__W16__	.10	__A04*__+A15+__H25*__+H13+H17→__H09__	.20
		__H13*__+H25+__A04*__→__H28__	.17
		__H17*__+__A04*__→__H13__	.16
		__H17*__+__A09*__+H09+A11→__H25__	.15
		__H17*__+H13+__A16*__→__H15__	.10
*Stronger ISP@W or ISP@H SRW and stronger ISA SRW			
Table 43			

Table 43 lists the composite explanations for retained formal and informal practices regressed over all applicable awareness measures ($p<.05$) and practice UIVs ($p<.05$). The relationships were ordered by SRWs and individual SRWs were omitted for table simplicity. The ISP@W measures showed that formal UIVs were stronger explanations than awareness. ISP@H measures also showed that informal UIVs were stronger explanations than awareness, with the exception of formal practice H09. For formal practice H09, technology awareness (A04) was the stronger explanation over user authentication (H25) when *reviewing virus protection software logs for scheduled updates and drive scans* (H09).

Contrasting awareness-to-practice relationships from Tables 40 and 43 showed the influence of formal and informal UIVs. Weaker and inverse awareness relationships diminished when stronger practice relationships were introduced, which yielded improved explanations for formal and informal practice. Practice UIVs also increased the average explained variance of a formal practice from .12 to .29 and an informal practice from .13 to .27. Therefore, formal and informal UIVs increased the average effect of ISA-to-practice relationships from medium to large.

From Table 43, policy awareness items (A06, A09, or A10) were absent from all ISA-to-ISP@W relationships. Explanations for formal practice variance yielded a unique domain substitution for the ISP@W construct, where policy awareness was substituted with deterrent-preventive effort. Formal practices W09 and W16 were combined deterrent-preventive efforts, which originated within security policy and technology use. The deterrent-preventive effort of *reviewing virus protection software logs for scheduled updates and drive scans* (W09) was included in nine (82%) of the eleven formal practice explanations. Deterrent-preventive effort W16 was not explained by effort W09, yet the formal practice of *storing email on client computers rather than the email server* (W16) also contained the policy and technology perspective. Therefore, deterrent-preventive efforts practiced within the formal environment yielded a stronger explanation than individual policy awareness measures.

Table 44 lists the composite explanations for retained informal practice measures regressed over all formal measures (p<.05) and informal UIVs (p<.05). Relationships were ordered by SRW and SRWs were omitted for table simplicity. Contrasting ISP@W-to-ISP@H relationships from Tables 42 and 44 showed the influence of informal UIVs. However, comparing ISA-to-ISP@H relationships (Tables 40 and 43) with ISP@W-to-ISP@H relationships (Table 44) delineated awareness and formal practice differences. As with inverse awareness relationships, inverse formal practice relationships diminished when stronger informal measures were introduced, which yielded improvement in explained informal practice variance. The difference in average explained variance was greater for ISA-to-ISP@H relationships (.13 versus .27) when compared to ISP@W-to-ISP@H relationships (.29 versus .37). Also, average ISA-to-ISP@H explanations improved from medium to large effects, while ISP@W-to-ISP@H explanations improved the average large-effect size. Therefore, formal practice was a better explanation for informal practice beyond awareness.

Among the ISP@W-to-ISP@H relationships, formal practice measures were the strongest, most common explanation for 67% of the informal measures and informal UIVs were strongest among the remainder. The strongest formal practice explanations were distributed over the formal ISA domain measures of deterrent efforts (18%), preventive efforts (40%), and deterrent-preventive efforts (18%). The strongest informal UIV explanations were distributed over the informal ISA domain measures of security management (20%), access control (7%), and encryption (7%). Therefore, formal practice had greater explanations for the average informal practice, where preventive efforts were the most common, strongest explanation. Furthermore, *reviewing virus protection software logs for scheduled updates and drive scans* (H09) was the strongest informal UIV explanation. However, *remotely connecting to other computers and sharing drives, printers, or files* (H13) was the stronger, most common informal UIV explanation.

MR Combined Practice Relationships by Effect Size

ISP@W-to-ISP@H Relationships	R_{adj}^{2}
W19*+**H17***+H09+H25→**H18**	.64
W15*+**H13***+H17 +W10→**H14**	.60
H09*+**W08***+W19→**H08**	.59
W23*+**H25***+H17+H09→**H22**	.52
H09*+**W10***+H13→**H10**	.45
W18*+W15+**H13***+H25→**H17**	.45
W04*+**H17***+H09+H25+H13→**H04**	.38
W15*+**H13***+W08+H25→**H35**	.35
W16*+**H13***+H17→**H15**	.29
H17*+**W14***+W15→**H13**	.25
W09*+ W19+**H17***+H13 →**H09**	.23
W19*+**H13***+H17+H09→**H11**	.21
H13*+**W16***+W10+W19+H25→**H28**	.21
H09*+**W10***+W19+W23→**H21**	.19
W23*+**H17***+W10+W16+H09→**H25**	.19

*Stronger ISP@W or ISP@H SRW

Table 44

Standardized Direct, Indirect, and Total Effects

From Appendix J, straight lines with single arrow heads (→) represented direct effects or causal effects (Kline, 1998) from the research model, where an unobserved variable acknowledged influence on another observed or unobserved variable. Also within the research model, indirect or mediator effects (Kline, 1998) involved variables (ISA, ISP@W, or ISP@H) that passed along causal effects from prior path relationships onto subsequent variables (ISP@W and/or ISP@H). The hypothesized relationship of each mediator variable controlled for the hypothesized common causes (PI and CSE or PI, CSE, and ISA, respectively). Thus a strong direct effect from a mediator variable rejected the hypothesis that the mediating relationship resulted from spurious association (Kline, 1998).

Standardized direct effects were listed within the hybrid model from Appendix J. Also, AMOS software calculated the indirect effects from PI, CSE, and ISA through mediating constructs (ISA and/or ISP@W) for both observed and unobserved variables (ISA, ISP@W, ISP@H, and ISA domain measures). Combining direct and indirect standardized effects yielded total standardized effects among the constructs of interest and ISA domain measures. Table 45 lists the standardized indirect effects estimated from the SEM results for the user-level ISA concept. Also, Table 46 lists the standardized total effects estimated from the SEM results for the user-level ISA concept.

Standardized indirect effects. From Table 45, both individual traits PI and CSE indirectly influenced practice constructs and ISA domain measures. However, PI and CSE offered the least influence on deterrent efforts practice. Also, PI and CSE were less indirect influences among ISP@W and other particular ISA domain measures. Furthermore, both PI and CSE were stronger indirect influences among the ISP@H construct and the individual threat-context awareness measures. Therefore, the mediator variables ISA and ISP@W yielded indirect PI and CSE relationships beyond spurious associations.

Individual ISA provided strong indirect influence over ISP@H and particular informal practice measures, where ISA was the strongest over informal access control practice. Therefore, the mediator variable ISP@W yielded indirect ISA relationships beyond spurious associations. Both ISA and ISP@W were strong indirect influences on ISA domain informal practice measures, with the strongest indirect influence on informal access control. However, ISA had the stronger indirect influence over informal practice measures. Therefore, the stronger ISA indirect influence resulted from strong mediation by ISP@W over ISP@H.

User-level ISA Concept Estimated Standardized Indirect Effects (p<.00)

Construct / ISA Domain Influenced	PI	CSE	ISA	ISP@W
ISP@H	0.28	0.27	**0.61**	
ISP@W	0.23	0.22		
Threat-context awareness	0.28	0.27		
Technology awareness	0.25	0.24		
Policy awareness	0.21	0.21		
Preventive efforts	0.20	0.20	**0.68**	
Deterrent-preventive efforts	0.20	0.19	**0.66**	
Deterrent efforts	0.13	0.13	**0.44**	
Access Control	0.24	0.23	**0.80**	**0.68**
Encryption	0.21	0.20	**0.70**	**0.59**
Security Management	0.20	0.20	**0.68**	**0.58**
User Authentication	0.19	0.18	**0.62**	**0.53**
Physical Protection	0.15	0.14	**0.50**	**0.42**

Large influence **Medium influence** Small influence

Table 45

Standardized total effects. Table 46 lists the combined standardized direct and indirect effects on each endogenous construct, ISA domain, and trait item-response variable. Each standardized total effect reflected influence from a respective research model construct (PI, CSE, ISA, ISP@W, and ISP@H). Also, each construct of interest was a large-effect explanation among the respective scale item-response or item subscales. A review of standardized total effects as construct influence follows.

Both individual trait constructs (PI and CSE) influenced individual ISA, ISP@W, ISP@H, and ISA domain measures. The power of the PI or CSE standardized total effects were 1.00 for effects greater than .20, and ranged from 0.99 to 0.71 for effects between .20 and .13. Trait constructs offered less influence among ISP@W and practice measures. In contrast, both PI and CSE offered more influence over individual ISA, ISP@H, and the individual ISA measures. Moreover, PI was consistently more influential than CSE over constructs and particular ISA domain measures.

User-level ISA Concept Estimated Standardized Total Effects (p<.00)

Construct, ISA Domain, or Trait influenced	ISA	ISP@W	ISP@H	PI	CSE
Individual ISA				0.30	0.29
ISP@W	**0.77**			0.23	0.22
ISP@H	**0.94**	**0.79**		0.28	0.27
Threat-context awareness	**0.94**			0.28	0.27
Technology awareness	**0.82**			0.25	0.24
Policy awareness	**0.71**			0.21	0.21
Preventive efforts	**0.68**	**0.88**		0.20	0.20
Deterrent-preventive efforts	**0.66**	**0.86**		0.20	0.19
Deterrent efforts	0.44	**0.57**		0.13	0.13
Access Control	**0.80**	**0.68**	**0.85**	0.24	0.23
Encryption	**0.70**	**0.59**	**0.75**	0.21	0.20
Security Management	**0.68**	**0.58**	**0.73**	0.20	0.20
User Authentication	**0.62**	**0.53**	**0.67**	0.19	0.18
Physical Protection	**0.50**	0.42	**0.53**	0.15	0.14
PI03…I seek out new ways to do things.				**0.83**	
PI02…I enjoy trying out new ideas.				**0.83**	
PI11…I am an inventive kind of person.				**0.75**	
PI01…my peers ask me for advice or information.				**0.73**	
PI05…I frequently improvise methods for solving a problem when an answer is not obvious.				**0.71**	
PI14…I find it stimulating to be original in my thinking and behavior.				**0.71**	
PI18…I am receptive to new ideas and practices.				**0.68**	
PI09…I consider myself to be creative and original in my thinking and behavior.				**0.66**	
PI12…I enjoy taking part in the leadership responsibilities of groups.				**0.66**	
PI19…I am challenged by unanswered questions.				**0.64**	
PI08…I feel that I am an influential member of my peer group.				**0.58**	
CSE04…if I had seen someone else using it before trying it myself?					**0.87**
CSE05…if I could call someone for help if I got stuck?					**0.87**
CSE07…if I had a lot of time for the completion of the task(s)?					**0.84**
CSE06…if someone else had helped me get started?					**0.82**
CSE08…if I had just the built-in help facility for assistance?					**0.82**
CSE03…if I had only manuals for reference?					**0.81**
CSE09…if someone showed me how to do it first?					**0.81**
CSE01…if there was no one around to tell me what to do as I go?					**0.79**
CSE10…if I had used similar applications before to obtain the same goal?					**0.77**
CSE02…if I had never used another application like it before?					**0.75**

Large influence **Medium influence** Small influence

Table 46

PI offered more consistent influence than CSE, except among the ISA domain measures that attempted to alter security behavior. Both PI and CSE equally influenced the ISA domain measures of policy awareness, preventive efforts, deterrent efforts, and security management. Within these ISA domain measures, decision-makers used policy or technology to alter security behavior. Conversely, PI was slightly more influential among the deterrent-preventive measures, which resulted when decision-makers incorporated both individual policy and technology awareness to alter security behavior.

Individual ISA offered strong influence over ISP@W and ISP@H, with the strongest influence (.94) over informal practice, which rivaled individual ISA influence over threat-context awareness measures. The power of the individual ISA standardized total effects were 1.00 across all constructs and ISA domain measures. The stronger individual ISA influence over informal practice ranged from access control (.80) to physical protection (.50). In contrast among formal practice, individual ISA offered strong influence over preventive efforts (.68) and deterrent-preventive efforts (.66), with weaker influence over deterrent efforts (.44). Also, formal practice (ISP@W) offered strong influence (.79 and power = 1.00) over informal practice (ISP@H), yet individual ISA consistently offered more influence for informal practice and among informal practice measures. Therefore, individual security awareness influenced practice within the informal environment more than practice within the formal environment. Moreover, individual ISA equally influenced threat-context awareness and informal security practice.

Explained and Unexplained Awareness and Practices

SEM hybrid model results from Appendix J identified explained (SMC) and unexplained (disturbance terms d1, d2, and d3) response variance among the endogenous research model constructs (ISA, ISP@W, and ISP@H). Also, construct explanations (SMC) among ISA domain measures implied additional unexplained research model response variance (1 – SMC).

Among the endogenous constructs and the path relationships identified from Appendix J, individual human traits (PI and CSE) explained 28% of individual ISA. Subsequently, PI, CSE, and individual ISA explained 7% of ISP@W. Also, the combined research model constructs PI, CSE, ISA, and ISP@W explained 60% of ISP@H. All construct explanations had sufficient power (1.00), where ISA and ISP@H explanations were large-effects and the ISP@W explanation was a small-effect. However, 72% of ISA, 93% of ISP@W, and 40% of ISP@H remained unexplained as illustrated by the exogenous disturbance terms d1, d2, and d3, respectively. Therefore, the research model explained a large majority of response variation within ISP@H, but left the majority of ISA and a larger majority of ISP@W response variations unexplained. Table 47 lists the explained and unexplained research model response variance for ISA, ISP@W, ISP@H, and ISA domain measures.

Individual ISA, ISP@W, and ISP@H constructs were large-effect explanations, with sufficient power (power=1.00), among the ISA domain measures from Table 47. However, the construct explanations implied that response variations were unexplained for particular research model domain measures of policy awareness (.50), deterrent efforts (.68), user authentication (.55), and physical awareness (.72). Therefore, the user-level ISA concept explanations among particular ISA domain measures of threat-context awareness, technology awareness, preventive efforts, deterrent-preventive efforts, access control, encryption, and security management sufficiently explained the majority of response variation. Furthermore, the majority of the user-level ISA concept response variation among policy awareness, deterrent efforts, user authentication, and physical protection were unexplained.

User-level ISA Concept Explained and Unexplained Response Variance

Construct	ISA Domain Measure	% Explained	% Unexplained
ISA	Threat-context awareness	88	12
% Explained: 28	Technology awareness	68	32
% Unexplained: 72	Policy awareness	50	50
ISP@W	Preventive efforts	77	23
% Explained: 7	Deterrent-preventive efforts	74	26
% Unexplained: 93	Deterrent efforts	32	68
	Access control	73	27
ISP@H	Encryption	56	44
% Explained: 60	Security management	53	47
% Unexplained: 40	User authentication	45	55
	Physical protection	28	72

Table 47

Overall, the research model and survey instrument explained 60% of the response variation among informal security practice, which required PI, CSE, individual ISA, and formal security practice. Also, PI, CSE, individual ISA, and formal practice explained the majority of preventive efforts and deterrent-preventive efforts. PI, CSE, individual ISA, formal practice, and informal practice explained the majority of access control, encryption, and security management measures. Lastly, PI, CSE, and individual ISA explained the majority of individual threat-context and technology awareness. However, the majority of policy awareness, formal security practice, and deterrent efforts were unexplained by individual traits and individual ISA. Furthermore, physical protection and user authentication measures also required explanation beyond individual traits, individual ISA, formal practice, and informal practice.

The three disturbance terms from Appendix J (d1, d2, and d3) indicated that other explanations for ISA, ISP@W, and ISP@H existed outside of the user-level ISA concept. Furthermore, the three disturbance term estimates were correlated, which equated to unanalyzed associations (Kline, 1998). Disturbance term pairings $d1_{ISA}\leftrightarrow d2_{ISP@W}$ and $d1_{ISA}\leftrightarrow d3_{ISP@H}$ were inversely correlated ($p<.00$). Hence, unexplained response variation from $d1_{ISA}$ corresponded with proportional common differences among unexplained response variations from $d2_{ISP@W}$ or $d3_{ISP@H}$. Also, disturbance term $d2_{ISP@W}$ and the PI construct were positively correlated ($p\leq.02$). Kline (1998) noted that correlation between disturbance terms and exogenous constructs implied the presence of an omitted variable, which was evident from the small-effect ISP@W explanation and the resulting large-effect disturbance term (d2). Therefore, the user-level ISA concept explained ISP@W with respect to ISP@H.

Measurement Error Variances and Correlations. As was previously noted within the CFA results; individual error terms were exogenous, one-dimensional, and independent measures. However, correlation between individual error terms identified unknown commonalities beyond the research model (Kline, 1998) and commonality among measurement error was observed within the hybrid model results. Appendix J omitted the exogenous error term variances for individual traits (CSE and PI), deterrent efforts, and physical protection, along with all error term correlations. Table 48 lists the omitted hybrid model estimated error term variances (p<.00).

SEM Estimated Error Variances for Item-Subscales and Individual Traits			
Item-response	Estimated Error σ^2	Item-response	Estimated Error σ^2
Deterrent Efforts	1.01		
Physical Protection	1.43	PI01	.67
CSE01	.62	PI02	.38
CSE02	.68	PI03	.37
CSE03	.44	PI05	.51
CSE04	.29	PI08	.62
CSE05	.25	PI09	.50
CSE06	.34	PI11	.47
CSE07	.33	PI12	.63
CSE08	.44	PI14	.45
CSE09	.34	PI18	.42
CSE10	.39	PI19	.52

Table 48

Tables 49a and 49b list correlated error terms between constructs and the estimated correlations among ISA-to-ISP@W and ISP@W-to-ISP@H measures, respectively. Also, Tables 49c, 49d, and 49e list correlated error terms from within constructs and the estimated correlations among respective ISA domain measures. Tables 49f and 49g list correlated error terms within trait constructs and the estimated correlations among CSE and PI measures, respectively. All of these correlated error terms from the hybrid model results were also identified in the CFA results. The same explanations from the CFA results apply to the hybrid model results.

User-level ISA Concept ISA-to-ISP@H Correlated Error Terms (p<.00)	
Correlated Error Terms	Estimated Correlation
technology awareness ↔ access control	**+0.25**
technology awareness ↔ security management	+0.22

Table 49a

User-level ISA Concept ISP@W-to-ISP@H Correlated Error Terms (p<.00)

Correlated Error Terms	Estimated Correlation
deterrent efforts ↔ user authentication	+0.35
preventive efforts ↔ encryption	**+0.54**
deterrent-preventive efforts ↔ physical protection	-0.18
deterrent-preventive efforts ↔ access control	**-0.41**

Table 49b

User-level ISA Concept Within-ISA Correlated Error Terms (p<.00)

Correlated Error Terms	Estimated Correlation
technology awareness ↔ threat-context awareness	**-0.78**

Table 49c

User-level ISA Concept Within-ISP@W Correlated Error Terms (p<.02)

Correlated Error Terms	Estimated Correlation
preventive efforts ↔ deterrent-preventive efforts	**-0.16**

Table 49d

User-level ISA Concept Within-ISP@H Correlated Error Terms (p<.00)

Correlated Error Terms	Estimated Correlation
access control ↔ user authentication	**-0.21**
access control ↔ security management	**+0.14**

Table 49e

User-level ISA Concept Within-CSE Correlated Error Terms (p<.00)

Correlated Error Terms	Estimated Correlation
CSE01 ↔ CSE02	**+0.74**
CSE01 ↔ CSE03	+0.34
CSE01 ↔ CSE09	-0.24
CSE02 ↔ CSE03	+0.34
CSE02 ↔ CSE09	-0.24
CSE04 ↔ CSE07	-0.25
CSE04 ↔ CSE08	**-0.32**
CSE05 ↔ CSE08	-0.28
CSE05 ↔ CSE06	+0.27
CSE06 ↔ CSE07	+0.22
CSE06 ↔ CSE09	+0.30
CSE09 ↔ CSE10	+0.42

Table 49f

User-level ISA Concept Within-PI Correlated Error Terms (p<.00)

Correlated Error Terms	Estimated Correlation
PI01 ↔ PI08	+0.15
PI01 ↔ PI02	+0.25
PI02 ↔ PI03	**+0.48**
PI08 ↔ PI09	+0.25
PI08 ↔ PI12	+0.20
PI09 ↔ PI14	+0.27
PI11 ↔ PI12	+0.26
PI11 ↔ PI14	+0.25
PI11 ↔ PI18	**-0.21**
PI12 ↔ PI14	+0.23

Table 49g

RQ2, RQ3, RQ4, RQ5, and RQ6 SEM Hybrid Model Supported Answers

SEM hybrid model results provided additional granularity for CFA answers to the second, third, and fourth research questions. Also, SEM hybrid model results answered the fifth and sixth research questions. This section reviews each research question, along with the answers from supporting hybrid model results.

What are measures of information security awareness (RQ2)? SEM standardized total effects identified constructs and ISA domain measures that were both strong measures of individual ISA. The domain measure of threat-context awareness and the informal practice construct were equally the strongest measures of individual ISA. Furthermore, access control measures were stronger among informal practice. MR analysis identified the most frequent informal practice relationship explanation was a technology awareness measure A04—*personal firewall software can block logical port access to/from a computer*. Also, preventive efforts measures were stronger among formal practice measures. MR analysis identified the most frequent ISA measure among formal practice relationship explanations was the threat-context awareness measure A18—*encryption can deter unauthorized access to sensitive information.*

The SEM hybrid path model results estimated that individual traits of PI and CSE explained 28% of the response variation across individual ISA. Therefore, all of the individual trait measures had varying influence on individual ISA. Among the PI measures, *seeking out new ways to do things* (PI03) had the stronger PI relationship. Also, among the CSE measures, *having seen someone else use security software before trying it* (CSE04) had the stronger CSE relationship.

Which information security practices reflect individual ISA (RQ3)? The hybrid model results identified direct individual ISA relationships between ISP@W and ISP@H (retained H1 and H2, respectively), as well as each practice construct's role as a moderator variable for individual ISA over the respective ISA domain measures. Also, MR analysis identified individual ISA measures among the relationships explanations for both formal and informal practice. Therefore, all formal and informal security practice reflects varying amounts of individual ISA from particular ISA domain measures.

SEM standardized total effects identified that individual ISA was a stronger influence over informal practice (.94) than formal practice (.77). However, the formal practice construct was the stronger direct measure of individual ISA (.77 versus .33). Formal practice mediated individual ISA over a strong direct ISP@W relationship with ISP@H (.79), which yielded the stronger ISA influence over informal practice. Also, the SEM model estimated individual ISA to explain from 64% (access control) to 19% (deterrent efforts) of the response variations among ISA domain practice measures.

MR analysis identified individual security practice relationships, which included both awareness items and practice items as explanations. However, MR analysis also identified that deterrent-preventive efforts replaced the ISA domain measure of individual policy awareness among ISA-to-ISP@W relationships within the ISP@W construct. The formal practice of *reviewing virus protection software logs for scheduled updates and drive scans* (W09) and *storing email on client computers rather than the email server* (W16) yielded stronger policy awareness than retained policy awareness items A06, A09, or A10.

<u>Do security practices differ between computing-environments (RQ4)?</u> The hybrid model results noted several differences between formal and informal security practice. 1) Formal practice was categorized as the appropriate use of policy and/or technology awareness, yet informal practice was categorized as the appropriate use of threat-context awareness. 2) Formal practice was a strong, direct influence on informal practice (retained H3). Also, individual ISA had the stronger, direct influence on formal practice (retained H1) versus informal practice (retained H2). However, informal practice mediated the stronger ISA total influence over informal practice. 3) The noted unobserved absence of individual ISA domain measures within each environment were supported from comparisons between MR analyses of ISA-to-practice relationships. As noted in RQ3, policy awareness measures were included among informal relationship explanations, yet preventive-deterrent measures were substituted for policy awareness among the formal relationship explanations. Furthermore, ISA-to-practice relationships identified threat-context awareness explanations among formal practice relationships compared to technology awareness explanations among informal practice relationships. 4) Lastly, the research model explained 60% of the response variation among informal practice, yet only 7% of the formal practice was explained. Therefore, the hybrid model

results highlighted different individual ISA deficiencies among security practice between environments. The known-groups results also provided more clarification to RQ4.

Does CSE influence individual ISA (RQ5)? From the hybrid model results, retained research hypothesis H5 substantiated that CSE did influence individual ISA with a small-effect explanation (8%). Furthermore, the SEM standardized indirect effects showed that individual ISA mediated CSE influence over ISA domain measures. The strongest CSE influence, beyond individual ISA, were small-effect explanations (7%) among the threat-context awareness measures and the informal practice construct. The weakest CSE influence (≈ 2%) was noted among the ISA domain measures of deterrent efforts and physical protection. Therefore, CSE did influence ISA with small-effect explanations among ISA, ISP@W, ISP@H, and ISA domain measures. Moreover, the stronger small effect CSE explanations were offered among informal practice, threat-context awareness, and technology awareness.

Does PI influence individual ISA (RQ6)? Similarly from the hybrid model results, retained research hypothesis H4 substantiated that PI did influence individual ISA with a medium-effect explanation (9%). The SEM standardized indirect effects showed that individual ISA also mediated PI influence, similar to CSE, which yielded small-effect explanations over ISA domain measures. As previously noted, PI had consistently more small-effect influence than CSE for practice constructs and particular ISA domain measures. Therefore, PI did influence ISA with a medium-effect explanation for individual ISA and small-effect explanations among ISP@W, ISP@H, and ISA domain measures. Furthermore, the strongest small-effect PI explanations were offered among informal practice, threat-context awareness, and technology awareness. Also, PI was positively correlated (ρ ≈ .14, p<.00) with formal practice disturbance (disturbance term d2). The d2↔PI correlation indicated that an unknown variable(s), outside the research model, was positively correlated with PI and the unexplained formal practice response variation.

Results of Known-groups Analysis

Known-groups analysis of PI, CSE, and ISA domain means provided additional answers to the fourth research question, as well as relationships and group mean differences among demographic and information technology variables. Analysis of variance (ANOVA) statistical techniques denoted ISA domain measures with mean differences over demographic and technology known-groups. ISA, ISP@W, and ISP@H were represented by item subscales measures. Also, PI and CSE were represented by an arithmetic average of each respective construct's scales.

All demographic and technology variables were categorical. The demographic variables were identified individually and organizationally from Chapter II (refer to table 8a). Differences between business (formal) and home (informal) computing-environments were also identified among information technology variables from Chapter II (refer to table 8b). The technology variables were grouped by hours-of-use (weekly hours of computer use and Internet use) and computer software/hardware configuration (type of operating system, local area network connection, and Internet connection). Multiple business computer locations used and the frequency of reported business computer locations were also included. Appendix G listed the survey response categories for each known-groups variable and Appendix K lists the response frequencies.

Known-groups analysis results yielded association statistics (eta-squared—η^2 or partial eta-squared—η_p^2) for explained variances among ISA domain measures. Also, graphs of known-groups effects ISA domain measures provided additional granularity among known-groups mean differences. Detailed known-groups results follow for individual demographics, organizational demographics, and technology variable comparisons between computing-environments. The section concludes with the supported answers to the fourth research question (RQ4).

Individual Demographic Variables

Individual demographic known-groups included respondent gender, education-level, age, and years-of-computer-use. One-way ANOVA results yielded mean differences ($p<.05$) among respective gender and education-level known-groups. However, one-way ANOVAs showed no mean differences among age or years-of-computer-use. Furthermore, multivariate analysis of variance (MANOVA) yielded associations ($p<.05$) among gender, education-level, age, years-of-computer-use, and interaction effects. Table 50 lists the one-way ANOVA results. Table 51 lists the MANOVA results.

ANOVA Results for Individual Demographic Known-groups

Factor	Dependent Variable	F-ratio	p-value	η^2	Power
Gender	CSE	34.36	.00	.06	1.00
	PI	26.24	.00	.05	1.00
	Technology	16.95	.00	.03	0.98
	Preventive	31.05	.00	.06	1.00
	Deterrent – Preventive	28.14	.00	.04	0.99
	Access Control	50.47	.00	.10	1.00
	User Authentication	11.47	.01	.01	0.81
	Security Management	55.21	.00	.08	1.00
	Encryption	53.37	.00	.08	1.00
Education-level	Preventive	2.35	.03	.03	0.81

Table 50

Individual demographic ANOVA results. The ISA domain measures of policy, threat-context, deterrent efforts, and physical protection had no mean differences (p<.05) with respect to gender. However, the other ISA domain measures listed in Table 50 had gender mean differences. Among all nine dependent variables, males had higher response means than females. The largest mean differences (MD≈0.6, p<.00) were among access control, security management, and encryption responses. The smallest mean differences (MD≈0.4, p<.00) were among personal innovativeness, deterrent-preventive efforts, and user authentication responses. Eight of the nine gender explanations were small effects, yet gender was a medium effect explanation (10%) for access control.

Education Level Effects on Preventive Efforts

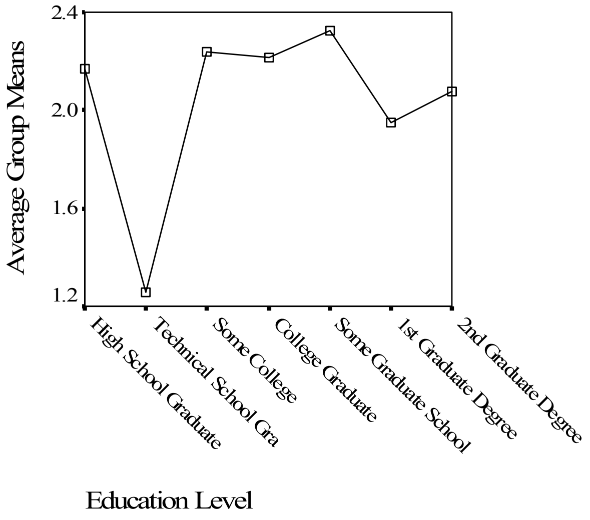


Figure 13

One-way ANOVA tests also showed that preventive efforts had education-level mean differences (p<.05). With respect to education levels listed in Appendix K, Technical School graduates averaged lower preventive efforts responses (p<.02) than other education-level groups. Moreover, Technical School graduates averaged lower responses (MD=.70, p<.00) than the overall preventive efforts response mean. Figure 13 depicts the education-level effects on preventive efforts.

Individual demographic MANOVA results. Groups are considered approximately equal if the largest group size divided by the smallest group size is less than 1.5 (Hair et al., 1998). For this study, female respondents (272) divided by male respondents (259) yielded a quotient of 1.1.

MANOVA Results for Individual Demographic Known-groups

Source	Dependent Variable	df	F-ratio	p-value	η_p^2	Power
Gender Wilks' Λ = .90 F-ratio = 6.51 P-value = .00 η_p^2 = .10 Power = 1.00	CSE	1	27.09	.00	.05	1.00
	PI	1	15.32	.00	.03	0.97
	Preventive Efforts	1	18.19	.00	.04	0.99
	Deterrent – Preventive	1	12.79	.00	.03	0.95
	Access Control	1	32.59	.00	.06	1.00
	Security Management	1	26.55	.00	.05	1.00
	Encryption	1	29.64	.00	.06	1.00
Education-level^ Wilks' Λ = .97 F-ratio = .92 p-value = .55 η_p^2 = .02 Power = .64	Preventive Efforts	2	3.08	.05	.01	.59
	Deterrent-Preventive	2	3.15	.04	.01	.60
G * E^ * A^ * Y^ Wilks' Λ = .44 F-ratio = 1.21 p-value = .01 η_p^2 = .10 Power = 1.00	CSE	43	1.55	.02	.12	1.00
	Deterrent Efforts	43	1.41	.05	.11	1.00
	Deterrent – Preventive	43	1.69	.01	.13	1.00

Table 51

Gender groups across ISA domain measures had equal variances. However, education-level, age, and years-of-computer-use known-groups had large-to-small group ratios beyond 1.5, which were suspect to unequal variances. Each of these factors was aggregated into three groups (low, medium, and high) with large-to-small group ratios less than 1.5. Appendix K referenced the aggregated known-groups for education-level^, age^, and years-of-computer-use^. Hence, education-level^, age^, and years-of-computer-use^ groups across ISA domain measures had equal variances.

The effects ($p<.05$) represented in Table 51 followed a reduced factorial model where gender, education-level^, age^, years-of-computer-use^, and the four-way interaction term explained 3% to 17% of response variation among ISA domain measures. Also, interaction effects rather than main effects attributed to the majority of explained variance (partial eta-squared—η_p^2). Table 51 also listed the univariate effects for gender, education-level^, and the interaction term (G * E^ * A^ * Y^).

Gender effects. With respect to the MANOVA results, gender was a small effect explanation for CSE, PI, preventive efforts, deterrent-preventive efforts, access control, security management, and encryption. Male respondents averaged higher responses than females for the respective ISA domain measures. Also, the univariate results corresponded with the previously reported one-way ANOVA results.

Education-level^ effects. Education-level^ had no significant multivariate effects, yet significant univariate effects were identified as small effect (1%) explanations for preventive efforts and deterrent-preventive efforts. Respondents with one graduate degree had lower preventive and deterrent-preventive responses than respondents with no graduate degree (MD=.25 and MD=.30 respectively, $p<.02$). Figure 14 depicts education-level^ effects on preventive efforts and deterrent-preventive efforts.

Education-level^ Effects

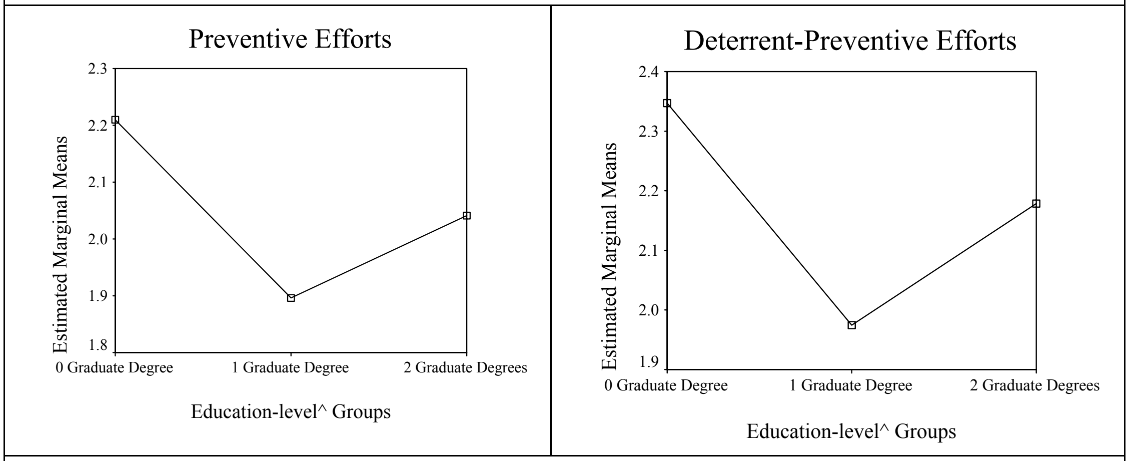


Figure 14

*Interaction effects (G*E^*A^*Y^).* Age^ and years-of-computer-use^ know-groups yielded no significant multivariate or univariate effects. However, group means decreased from low to medium age^ among CSE, deterrent efforts, and deterrent-preventive efforts. Also, the same ISA domain measure means increased from low to medium years-of-computer-use^. Moreover, CSE means increased over low to medium to high years-of-computer-use^. Age^ and years-of-compute-use^ known-groups for particular gender and education-level^ groups explained the G*E^*A^*Y^ effects. The four-way interaction term yielded medium effect explanations. Further analysis of the interaction term effects on CSE, deterrent efforts, and deterrent-preventive efforts follow.

*Interaction effects (G*E^*A^*Y^) on CSE.* With respect to CSE, the largest four-way interaction term (FWIT) group mean was for males with low education-level^, low age^, and high years-of-computer-use^. The smallest FWIT group mean was for females with high education-level^, medium age^, and low years-of-computer-use^. The mean difference (p<.00) between these extremes was 2.09. Figure 15 depicts the FWIT group means and G*E^*A^*Y^ effects on CSE.

Four-way Interaction Effects Group Means | CSE

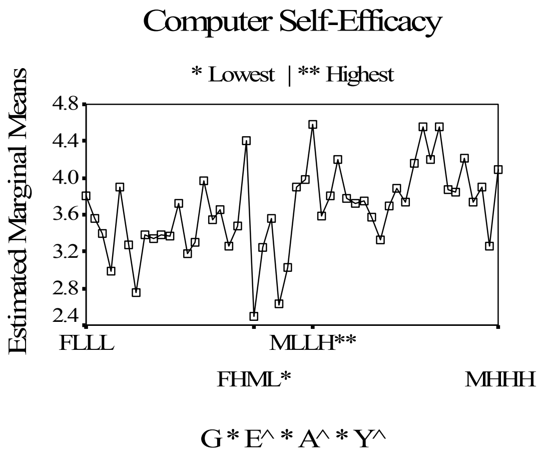


Figure 15

With respect to the FWIT group means, the largest CSE mean difference among female respondents (MD=1.90, p<.01) was high education-level^, low age^, and high years-of-computer-use^ versus high education-level^, medium age^, and low years-of-computer-use^. The least CSE mean difference among female respondents (MD=0.63, p<.04) was medium education-level^, low age^, and low years-of-computer-use^ versus low education-level^, high age^, and low years-of-computer-use^.

Figure 16 depicts CSE mean responses over age^ and years-of-computer-use^ known-groups for females with low education-level^. The CSE increase as years-of-computer-use^ increased was not significant (p<.43). However, the CSE decrease as age^ increased was a small effect explanation (R^2 = .10, R_{adj}^2 = .08, p<.00). Females with medium or high education-level^ had no significant age^ or years-of-computer-use^ mean difference.

Four-way Interaction Effect Explanation | Females – CSE

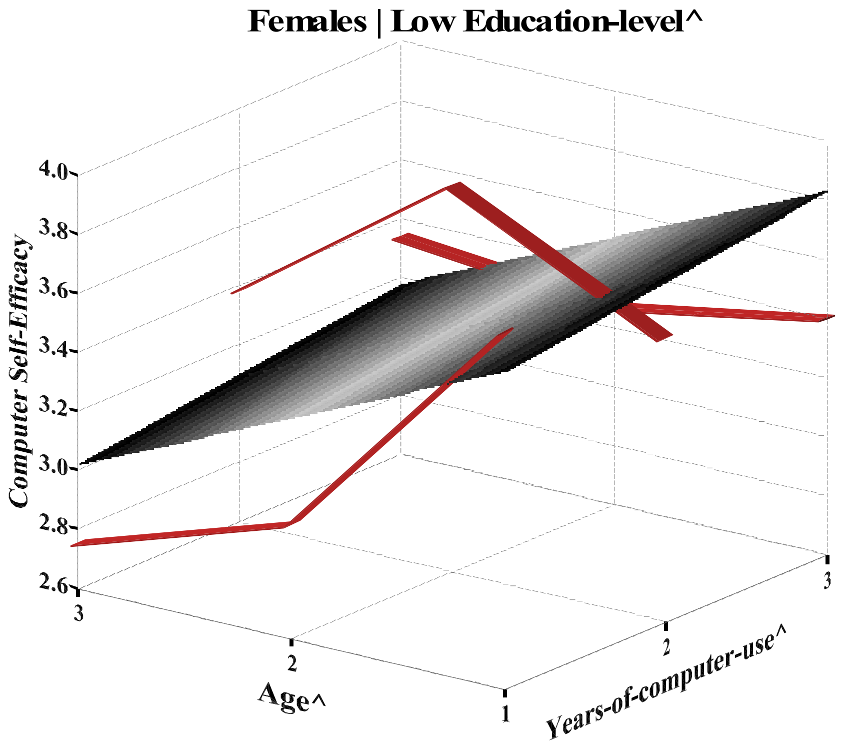


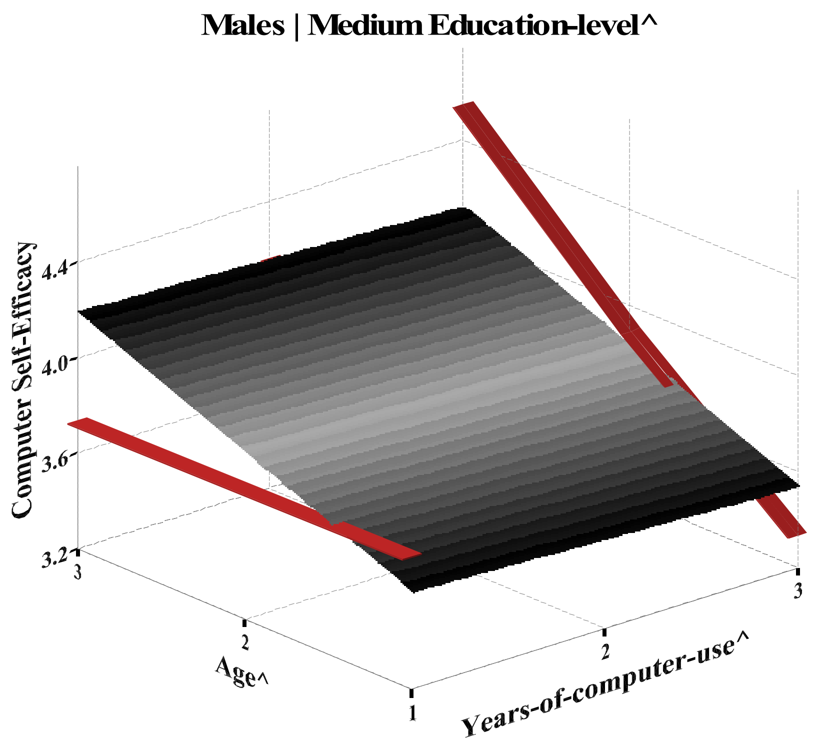
Figure 16

The largest CSE mean difference among males (MD=1.33, p<.01) was low education-level^, low age^, and high years-of-computer-use^ versus high education-level^, high age^, and medium years-of-computer-use^. The least CSE mean difference among male respondents (MD=0.63, p<.04) was medium education-level^, low age^, and low years-of-computer-use^ versus low education-level^, high age^, and low years-of-computer-use^.

Figure 17 depicts CSE mean responses over age^ and years-of-computer-use^ known-groups for males with medium education-level^. The CSE decrease as years-of-computer-use^ increased was not significant (p<.80). However, the CSE increase as age^

increased was a small effect explanation ($R^2 = .06$, $R_{adj}^2 = .03$, $p<.05$). Males with low or high education-level^ had no significant age^ or years-of-computer-use^ mean difference.

Four-way Interaction Effect Explanation | Males – CSE



Males | Medium Education-level^

Figure 17

*Interaction effects (G*E^*A^*Y^) on Deterrent Efforts.* With respect to deterrent efforts, the highest FWIT group mean was for males with low education-level^, high age^, and low years-of-computer-use^. The lowest FWIT group mean was for males with medium education-level^, high age^, and low years-of-computer-use^. The mean difference (p<.01) between these extremes was 2.17. Figure 18 depicts the FWIT group means and the G*E^*A^*Y^ effects on deterrent efforts.

Four-way Interaction Effects Group Means | Deterrent Efforts

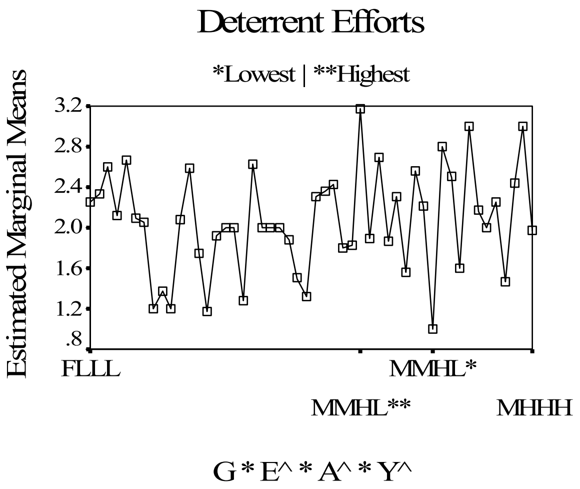


Figure 18

Based on the FWIT group means, the greatest deterrent efforts mean difference among female respondents (MD=1.50, p<.01) was observed between low education-level^, medium age^, and medium years-of-computer-use^ versus medium education-level^, medium age^, and medium years-of-computer-use^. The least deterrent efforts mean difference among female respondents (MD=0.73, p<.05) was low education-level^, high age^, and low years-of-computer-use^ versus medium education-level^, high age^, and high years-of-computer-use^.

Figure 19 depicts deterrent efforts means over age^ and years-of-computer-use^ for females with high education-level^. Females with medium or low education-level^ had no significant age^ or years-of-computer-use^ mean difference. The deterrent efforts decrease as years-of-computer-use^ increased was significant (p<.05). Also, the deterrent efforts increase as age^ increased was significant (p<.01). Both age^ and years-of-computer-use^ known-groups for females with high education-level^ provided a medium effect deterrent efforts explanation (R^2 = .18, R_{adj}^2 = .16, p<.00).

Four-way Interaction Effect Explanation | Females – Deterrent Efforts

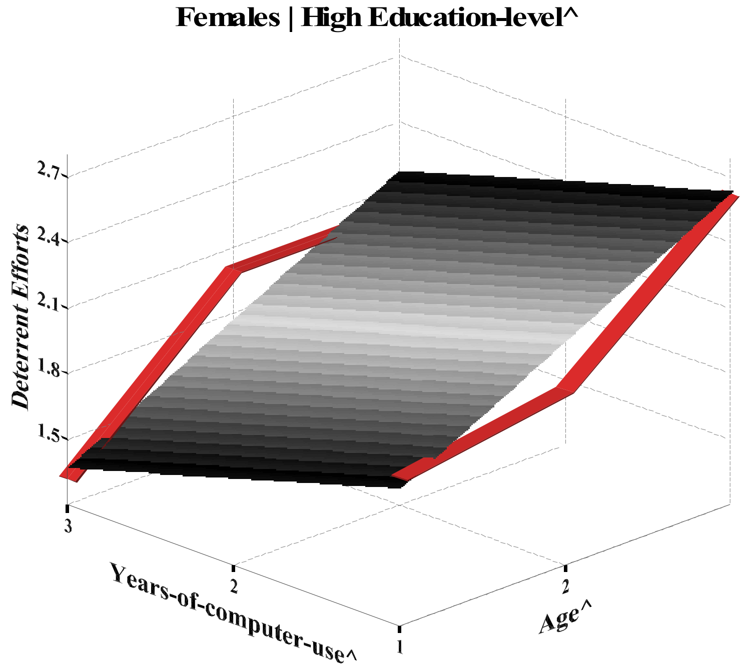


Figure 19

The greatest deterrent efforts mean difference among males (MD=2.17, p<.01) was previously noted. The least deterrent efforts mean difference among male respondents (MD=0.84, p<.05) was with low education-level^, low age^, and low years-of-computer-use^ versus high education-level^, medium age^, and high years-of-computer-use^. Males with low, medium, or high education-level^ had no significant age^ and/or years-of-computer-use^ associations with deterrent efforts.

*Interaction effects (G*E^*A^*Y^) on deterrent-preventive efforts.* With respect to deterrent-preventive efforts, the highest FWIT group mean was for males with high education-level^, high age^, and high years-of-computer-use^. The lowest FWIT group mean was for males with medium education-level^, high age^, and low years-of-computer-use^. The mean difference (p<.00) between these extremes was 2.75. Figure 20 depicts the FWIT group means and G*E^*A^*Y^ effects on deterrent-preventive efforts.

Based on the FWIT group means, the greatest deterrent-preventive efforts mean difference among female respondents (MD=1.77, p<.00) was observed between low education-level^, medium age^, and medium years-of-computer-use^ versus medium education-level^, medium age^, and medium years-of-computer-use^. The least deterrent-preventive efforts mean difference among female respondents (MD=0.78, p<.01) was low education-level^, low age^, and low years-of-computer-use^ versus high education-level^, high age^, and high years-of-computer-use^. Females with low, medium, or high education-level^ had no significant (p≤.05) age^ and/or years-of-computer-use^ associations with deterrent-preventive efforts.

Four-way Interaction Effects Group Means | Deterrent-Preventive

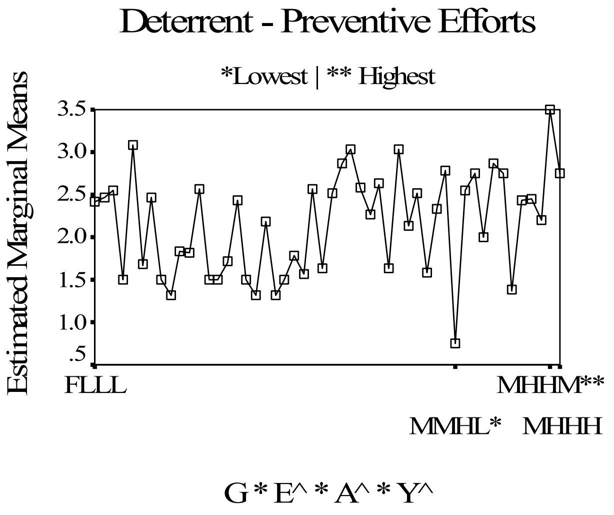


Figure 20

The greatest deterrent-preventive efforts mean difference among males (MD=2.75, p<.00) was previously noted. The least deterrent-preventive efforts mean difference among male respondents (MD=0.90, p<.05) was with low education-level^, low age^, and low years-of-computer-use^ versus low education-level^, high age^, and medium years-of-computer-use^. Males with low, medium, or high education-level^ also had no significant age^ and/or years-of-computer-use^ associations with deterrent-preventive efforts.

Organizational Demographic Variables

Organizational demographic variables were university area and job-type. Area and job-type known-groups had large-to-small group ratios beyond 1.5, which were suspect to unequal variances. Hence, dependent variables that failed the Levine's Test of Equality of Error Variances (H_0: $\sigma^2 = \sigma^2$) were omitted from ANOVA/MANOVA results.

ANOVA Results for Organizational Demographic Known-groups

Factor	Dependent Variable	(H_0: $\sigma^2 = \sigma^2$)	F-ratio	p-value	η^2	Power
Area	PI	p-value ≈.54	1.97	.02	.06	0.96
	Access Control	p-value ≈.46	2.41	.01	.06	0.98
	User Authentication	p-value ≈.14	2.18	.01	.06	0.98
	Security Management	p-value ≈.67	2.32	.00	.07	0.99
Job-Type	Threat-context	p-value ≈.27	2.70	.05	.02	0.66
	Deterrent-Preventive	p-value ≈.17	3.06	.03	.02	0.72

Table 52

One-way ANOVA results yielded mean differences (p<.05) among particular university area and job-type known-groups for ISA domain measures of threat-context, deterrent-preventive, access control, user authentication, and security management. Furthermore, MANOVA yielded association (Wilks' Λ = .88, F-ratio = 1.45, η_p^2 = .06, p<.03, and power = 1.00) among area known-groups for access control group means

(F-ratio = 1.92, η_p^2 = .06, p<.02, and power = .95). Job-type and the interaction effects lacked multivariate significance. Table 52 lists the one-way ANOVA results for area and job-type.

ANOVA results from Table 52 identified job-type known-groups as small-effect explanations for threat-context and deterrent-preventive efforts. The one-way ANOVA results also identified particular job-type mean differences (p<.05) across the individual ISA and ISP@W measures.

Job-Type Effects on Threat-context and Deterrent-Preventive Efforts

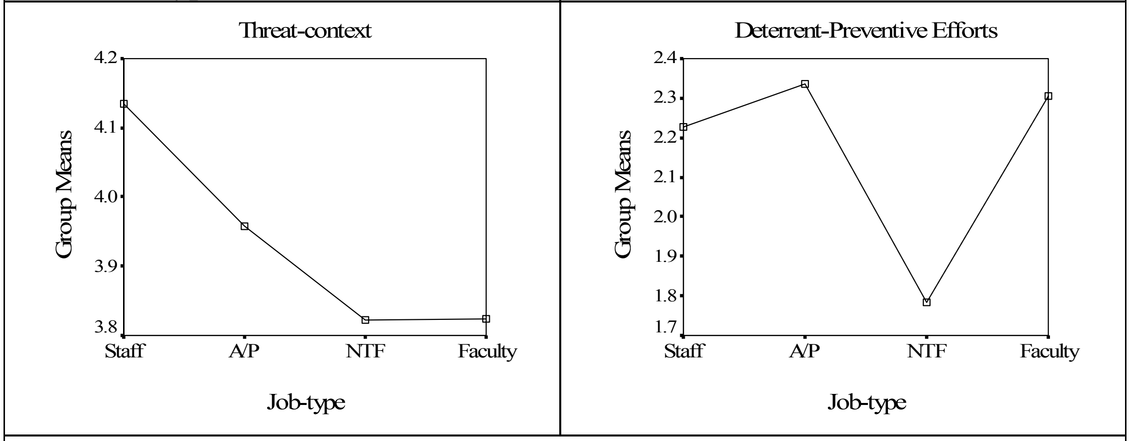
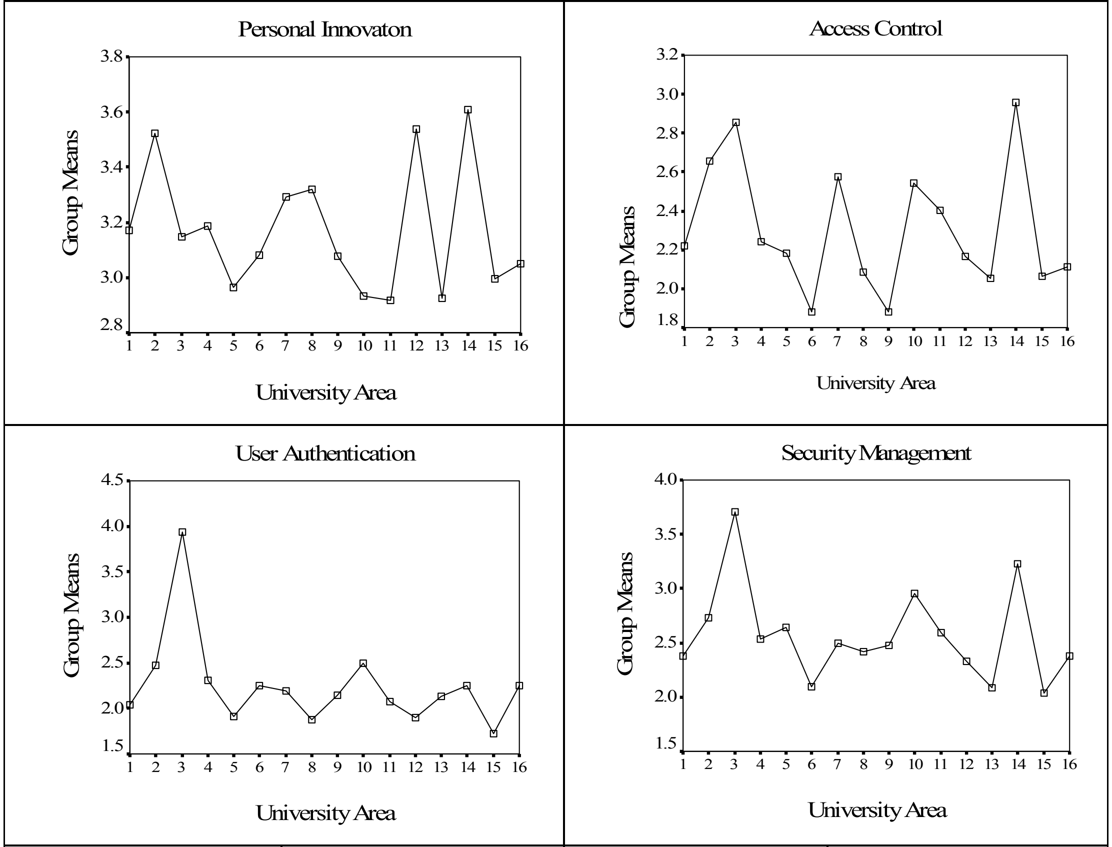


Figure 21

Figure 21 depicts the job-type group means as job-type effects across threat-context and deterrent-preventive efforts responses. Academic/professionals (A/P) employees had higher deterrent-preventive efforts mean responses (MD=0.55, p<.02) than non-tenured faculty (NTF) employees. Also, tenure-track faculty employees had higher deterrent-preventive efforts mean responses (MD=0.52, p<.05) than NTF employees. Staff employees averaged higher threat-context responses (MD=0.31, p<.05) than tenure-track faculty.

University Area Effects



1 – Administration	5 – Business	9 – Graduate School	13 – Outreach
2 – Agriculture	6 – Education	10 – Human Sciences	14 – Pharmacy
3 – AAES	7 – Engineering	11 – Liberal Arts	15 – COSAM
4 – ACES	8 – Forestry & Wildlife	12 – Nursing	16 – Veterinary Medicine

Figure 22

Figure 22 depicts the university area known-groups effects across PI, access control, user authentication, and security management responses. ANOVA results from Table 52 identified university area known-groups as small effect explanations for PI, access control, user authentication, and security management responses. Also, the PI trait and ISP@H measures had mean differences (p<.05) across university areas. The largest mean difference (MD=2.22, p<.00) was higher user authentication mean responses from the Alabama Agricultural Experiment Stations (AAES) respondents versus the College of

Science and Mathematics (COSAM) respondents. Also, AAES averaged higher security management responses (MD=1.67, p<.00) than COSAM. Pharmacy School respondents averaged higher access control responses (MD=1.08, p<.01) than Graduate School or College of Education respondents. Lastly, Pharmacy School respondents also had higher PI mean responses (MD=0.69, p<.00) than the College of Liberal Arts respondents.

Technology Variables

Technology variables were categorized as hours-of-use and hardware/software. Hours-of-use known-groups were identified as weekly hours of computer use and weekly hours of Internet use. Hardware/software known-groups were identified as computer operating systems, type of local-area-network (LAN) connection, and type of Internet connection. Survey respondents identified each of these technology variables with respect to their business (formal) computing-environment and home (informal) computing-environment. In addition, survey respondents identified multiple business computer locations, which indicated multiple business computer use. Detailed known-groups analysis follows for each hours-of-use and hardware/software variable.

Hours-of-use. Hours-of-use known-groups had large-to-small group ratios beyond 1.5, which were suspect to unequal variances. Therefore, the categories among weekly computer use and weekly hours of home Internet use were each aggregated into three separate groups (low, medium, and high use). Also, the categories among weekly hours of business Internet use were aggregated into two separate groups (low and high use). The aggregated hours-of-use^ known-groups were referenced in Appendix K.

MANOVA/ANOVA Results for Hours-of-use Known-groups

Weekly Hours-of-use	Dependent Variable	F-ratio	p-value	η_p^2	Power
Formal Computer^	PI	4.58	.01	.02	0.78
Informal Computer^ Wilks' Λ = .75 F-ratio = 6.09 p-value = .00 η_p^2 = .13 Power = 1.00	CSE	20.75	.00	.07	1.00
	PI	12.64	.00	.05	1.00
	Technology	13.98	.00	.05	1.00
	Threat-context	3.54	.03	.01	0.66
	Preventive Efforts	8.70	.00	.03	0.97
	Deterrent – Preventive	3.81	.02	.01	0.69
	Access Control	**45.53**	**.00**	**.15**	**1.00**
	Physical Protection	16.59	.00	.06	1.00
	User Authentication	8.03	.00	.03	0.96
	Security Management	**30.05**	**.00**	**.10**	**1.00**
	Encryption	23.17	.00	.08	1.00
Formal Internet^ Wilks' Λ = .79 F-ratio = 10.55 p-value = .00 η_p^2 = .21 Power = 1.00	CSE	3.89	.05	.01	0.50
	PI	16.56	.00	.03	0.98
	Technology	7.49	.01	.01	0.78
	Policy	30.99	.00	.06	1.00
	Threat-context	24.90	.00	.05	1.00
	Deterrent Efforts	28.06	.00	.05	1.00
	Preventive Efforts	23.02	.00	.04	1.00
	Deterrent – Preventive	**69.53**	**.00**	**.12**	**1.00**
	User Authentication	5.02	.03	.01	0.61
Informal Internet^ Wilks' Λ = .78 F-ratio = 5.24 p-value = .00 η_p^2 = .12 Power = 1.00	CSE	15.57	.00	.06	1.00
	PI	12.81	.00	.05	1.00
	Technology	11.41	.00	.04	0.99
	Threat-context	3.40	.03	.01	0.64
	Preventive Efforts	9.34	.00	.03	0.98
	Access Control	**36.64**	**.00**	**.12**	**1.00**
	Physical Protection	12.08	.00	.04	1.00
	User Authentication	8.70	.00	.03	0.97
	Security Management	**27.09**	**.00**	**.09**	**1.00**
	Encryption	18.12	.00	.06	1.00

Table 53

Table 53 lists the ANOVA results, which yielded mean differences ($p<.05$) among particular hours-of-use^ known-groups. Moreover, ANOVA results identified formal Internet, informal computer, and informal Internet hours-of-use^ known-groups as medium effect explanations for deterrent-preventive efforts, access control, and security management. Furthermore, Table 53 lists the MANOVA results that supported multivariate effects from the respective formal and informal hours-of-use^ known-groups, with no significant interaction effects.

Hours-of-use^ Effects

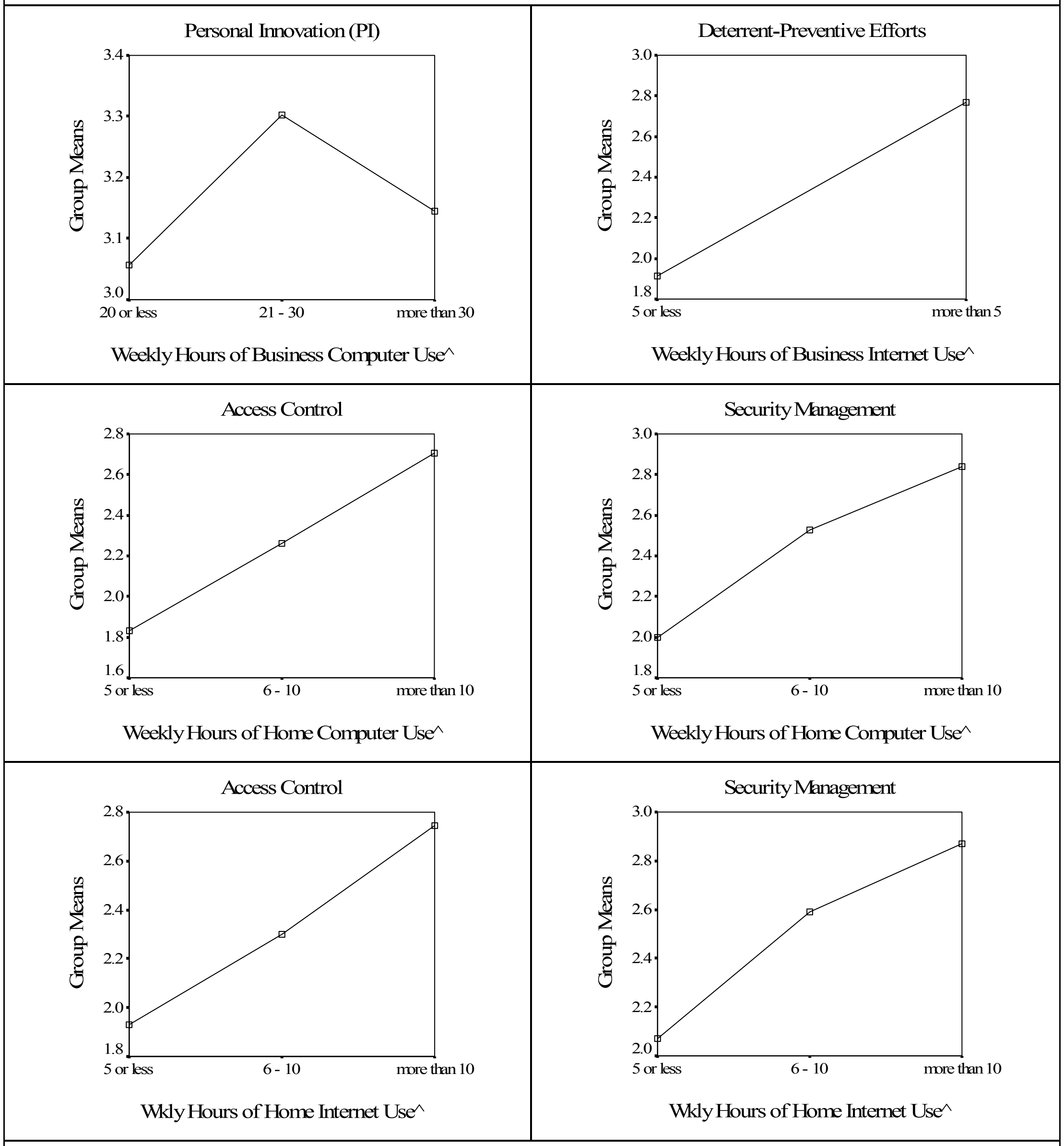


Figure 23

Figure 23 depicts the small (PI) and medium effect explanations across PI, deterrent-preventive efforts, access control, and security management responses. These medium-to-small effects were also the highest mean differences among hours-of-use^ known-groups. With respect to these ISA domain measures, the measures' means increased as informal hours-of-use^ categories increased. Likewise, the measure means increased as formal hours-of-use^ group categories increased.

Hours-of-use effects on PI. PI had the highest mean difference (MD=0.25, p<.01) among weekly hours of business computer use^. Employees who reported 20-30 hours per week on business computer use had higher PI mean responses than employees who reported less than 20 hours per week.

Hours-of-use effects on deterrent-preventive efforts. Deterrent-preventive efforts had the highest mean difference (MD=0.86, p<.00) among weekly hours of business Internet use^. Employees who reported more than five hours per week on business Internet use averaged higher deterrent-preventive efforts responses than employees who reported five hours or less per week.

Hours-of-use effects on access control and security management. Access control had the highest mean difference (MD=0.88, p<.00) among weekly hours of home computer use^. Employees who reported more than ten hours per week on home computer use averaged 1) higher access control responses than employees who reported five hours or less per week, and 2) higher access control responses (MD=0.44, p<.00) than employees who reported six to ten hours per week. Also, employees who reported six to ten hours per week on home computer use averaged higher access control responses (MD=0.43, p<.00) than employees who reported five hours or less per week

Security management also had a high mean difference (MD=0.84, p<.00) among weekly hours of home computer use^. Employees who reported more than ten hours per week on home computer use averaged 1) higher security management responses than employees who reported five hours or less per week, and 2) higher security management responses (MD=0.31, p<.02) than employees who reported six to ten hours per week. Likewise, employees who reported six to ten hours per week on home computer use averaged higher security management responses (MD=0.53, p<.00) than employees who reported five hours or less per week.

Lastly, access control (MD=0.81, p<.00) and security management (MD=0.80, p<.00) had the highest mean differences among weekly hours of home Internet use^. Employees who reported more than ten hours per week on home Internet use 1) averaged higher access control responses and 2) average higher security management responses than employees who reported five hours or less per week. In addition, employees who reported more than ten hours per week on home Internet use also 3) averaged higher access control responses (MD=0.44, p<.00) than employees who reported six to ten hours per week. Likewise, employees who reported six to ten hours per week of home Internet use 4) averaged higher access control responses (MD=0.37, p<.00) than employees who reported five hours or less per week.

Hardware/software. The hardware/software known-groups frequencies (refer to Appendix K) were skewed toward particular hardware/software configurations (i.e. Windows XP operating system, hub router LAN, and cable Internet connection) or a lack of knowledge about the configuration (i.e. I do not know.). Therefore, hardware/software known-groups had extreme large-to-small group ratios beyond 1.5, which were suspect to unequal variances. Hence, dependent variables that failed the

Levine's Test of Equality of Error Variances (H_0: $\sigma^2 = \sigma^2$) were omitted from further known-groups analysis.

ANOVA Results for Hardware/Software Known-groups

Factor	Dependent Variable	(H_0: $\sigma^2 = \sigma^2$)	F-ratio	p-value	η^2	Power
OS (F)	Preventive Efforts	p-value ≈ .06	2.04	.04	.03	0.83
OS (I)	CSE	p-value ≈ .14	5.08	.00	.08	1.00
	Threat-context	p-value ≈ .23	2.81	.00	.05	0.96
	User Authentication	p-value ≈ ..14	2.79	.00	.05	0.96
	Encryption	p-value ≈. 16	3.02	.02	.05	0.97
LAN (F)	PI	p-value ≈ .13	11.60	.00	.06	1.00
	Access Control	**p-value ≈ .86**	**22.02**	**.00**	**.11**	**1.00**
	Physical Protection	p-value ≈ .53	14.47	.00	.08	1.00
	Security Management	p-value ≈ .19	13.51	.00	.07	1.00
	Encryption	**p-value ≈ .30**	**32.46**	**.00**	**.16**	**1.00**
LAN (I)	PI	p-value ≈ .37	5.62	.00	.03	0.94
	Technology	p-value ≈ .05	13.69	.00	.07	1.00
	Policy	p-value ≈ .12	7.93	.00	.05	1.00
	Access Control	**p-value ≈ .28**	**16.27**	**.00**	**.09**	**1.00**
	Physical Protection	p-value ≈ .07	5.96	.00	.03	0.96
	Security Management	p-value ≈ .89	11.42	.00	.06	1.00
IC (F)	PI	p-value ≈ .89	5.93	.00	.04	0.99
	Policy	**p-value ≈ .09**	**13.64**	**.00**	**.09**	**1.00**
	Threat-context	**p-value ≈ .21**	**11.78**	**.00**	**.09**	**1.00**
	Deterrent Efforts	p-value ≈ .37	5.60	.00	.04	0.98
	Physical Protection	p-value ≈ .31	3.65	.01	.03	0.89
	Encryption	p-value ≈ .25	9.89	.00	.07	1.00
IC (I)	CSE	p-value ≈ .73	3.14	.01	.04	0.92
	Technology	p-value ≈ .34	6.67	.00	.07	1.00
	Deterrent Efforts	p-value ≈ .14	4.05	.01	.04	0.97
	Deterrent-Preventive	p-value ≈ .05	4.00	.00	.04	0.97
	Physical Protection	p-value ≈ .55	6.76	.00	.07	1.00
BCF (I)	Security Management	p-value ≈ .95	2.532	.01	.03	0.88

(F) = Formal / (I) = Informal

Table 54

The hardware/software known-groups were operating systems, LAN type, Internet connection type, and business computer locations. Table 54 lists the ANOVA results for these known-groups, which identified medium effect explanations for policy, threat-context, access control, and encryption. The remaining dependent variable results were small effect explanations. Further discussion for each of the hardware/software known-groups follows.

Operating systems (OS). Appendix K referenced that the majority of respondents had Windows XP at work (79%) and at home (76%). The ANOVA results from Table 54 yielded small effect explanations and mean differences (p<.05) among particular OS in both computing-environments. Preventive efforts had the highest mean difference (MD=.89, p<.02) between MAC users and respondents who did not have a business computer. Similarly, preventive efforts also had a high mean difference (MD=.57, p<.03) between Windows XP users and respondents who did not have a business computer.

Computer OS are identified on system boot-up, yet mean differences existed between particular home OS users and respondents who did not know their home computer OS. The latter group maintained the lower group mean. CSE had the highest mean difference (MD=2.44, p<.00) with Linux users. Also, CSE had similar high mean differences (p<.02) from MAC users, Windows ME users, Windows 2000 users, Windows XP users, and respondents without home computers. Similarly, threat-context had high mean differences (MD=2.16, p<.01) from Linux users, as well as mean differences (p<.04) from Windows 98 users, Windows NT users, Windows ME users, Windows NT users, and respondents without home computers.

Mean differences also existed between particular home OS users and respondents who did not own a home computer. The latter group also had the lower group mean. Encryption had the highest mean difference (MD=2.29, p<.04) with Linux users. Also, encryption had similar high mean differences (p<.03) from Windows 98, Windows ME, and Windows XP users. Likewise, user authentication had the same situational high mean differences (MD=1.37, p<.02) from Windows 98 users, as well as mean differences (p<.03) from Windows 2000 and Windows NT users.

Local-area-network connections (LAN). Wired or wireless local-area-network access was available to employees within the business computing-environment (Auburn University, 2006a; 2006b). However, Appendix K referenced that respondents were unaware of their LAN connection at work (61%) or at home (21%). The ANOVA results from Table 54 yielded mean differences (p<.05) among particular LAN connectivity groups in both computing-environments. Respondents who did not know their LAN connectivity type had the lower group means among all the significant ANOVA results.

LAN known-groups in the business computing-environment offered medium effect explanations among encryption (16%) and access control (11%) responses, as well as small effect explanations among PI, physical protection, and security management. Wired LAN connectivity (hub routers) had the higher mean differences (MD=1.04 and .70 respectively, p<.00) for encryption and access control. The lack of LAN connectivity (none) had the higher mean differences for PI (MD=.48, p<.01), physical protection (MD=1.34, p<.00), and security management (MD=.68, p<.00).

LAN known-groups in the home computing-environment also offered a medium effect explanation among access control (9%) responses, as well as small effect explanations among PI, technology, policy, physical protection, and security management. Hub routers had the higher mean differences (MD=.69, .37, .77, and .47 respectively, p<.00) for access control, PI, physical protection, and security management. The lack of LAN connectivity (none) had the higher mean differences (MD=.77 and .72 respectively, p<.00) for technology and policy.

Internet connection (IC). Within the business computing-environment, Internet connectivity was available to employees through network access (wired or wireless) or dial-up access (Auburn University, 2006a; 2006b). However, Appendix K referenced that respondents were unaware of their Internet connection at work (23%) or at home (3%). Appendix K also referenced that 95% of the respondents subscribed to home Internet connectivity, with the majority reported as Broadband (60% cable and 20% DSL). The ANOVA results from Table 54 yielded mean differences (p<.05) among particular Internet connectivity groups in both computing-environments.

Internet connectivity groups within the business computing-environment offered medium effect (9%) explanations for policy and threat-context responses, as well as small effect explanations for PI, deterrent efforts, physical protection, and encryption. Unaware users had lower mean responses than wired users for policy (MD=.90, p<.00), threat-context (MD=.63, p<.00), encryption (MD=.67, p<.00), deterrent efforts (MD=.47, p<.00), and PI (MD=.36, p<.00). Unaware users also had lower mean responses than users without Internet connectivity for physical protection (MD=.70, p<.05).

Home Internet connectivity groups offered small-effect explanations for CSE, technology, deterrent efforts, deterrent-preventive efforts, and physical protection. Unaware subscribers (do not know) or respondents without home computers (N/A) had lower mean responses than subscribers with Internet connectivity or users who chose not to subscribe to Internet connectivity (None).

With respect to CSE, DSL subscribers (MD=.97, p<.00), dial-up subscribers (MD=.96, p<.01), and cable subscribers (MD=.93, p<.00) had higher mean responses than unaware subscribers. With respect to technology, dial-up subscribers (MD=1.27, p<.00), cable subscribers (MD=1.16, p<.00), and DSL subscribers (MD=1.01, p<.00) had higher mean responses than respondents without home computers. Also with respect to technology, dial-up subscribers (MD=1.20, p<.00), cable subscribers (MD=1.10, p<.00), and DSL subscribers (MD=.94, p<.01) had higher mean responses than unaware subscribers.

Users without Internet connectivity (MD=1.81, p<.01) and dial-up subscribers (MD=1.03, p<.04) had higher deterrent efforts responses than respondents without home computers. Also, users without Internet connectivity (MD=1.72, p<.02) had higher deterrent efforts responses than unaware subscribers. Similarly, dial-up subscribers (MD=1.19 and 1.16 respectively, p<.01) had higher deterrent-preventive efforts responses than unaware subscribers and respondents without home computers.

Internet subscribers that knew the type of Internet connectivity and users without Internet subscriptions had higher physical protection mean responses than unaware subscribers. The highest mean differences (MD=2.19, p<.01) was from satellite and dial-up subscribers. DSL subscribers (MD=2.07, p<.0) and users without subscriptions ((MD=1.94, p<.02) had higher mean differences. The lower mean difference (MD=1.87, p<.00) was from cable subscribers.

Business computer location frequency (BCF). Respondents reported computer use across multiple locations within the business computing-environment. Appendix K referenced that 94% of the respondents used the office location for business computer use. Nonetheless, 59% of respondents reported other campus locations for business computing. The ANOVA results from Table 54 supported the number of reported business computer locations as a small effect (3%) explanation for security management.

The ANOVAs also yielded security management mean differences (p<.05) among reported frequencies of business computer locations.

Respondents who reported the use of five locations had higher security management mean responses than respondents who reported none, two, three, or four. The largest mean difference (MD=1.20, p<.02) was from none. Two (MD=.74, p<.04) and four (MD=.75, p<.04) reported locations also had large mean differences. The least mean difference (MD=.64, p<.05) was from three reported locations.

Known-groups Supported Answers to RQ4

The known-groups results supported several differences among security practices between formal and informal computing-environments. Table 55 summarizes the demographic and technology known-groups effects on ISP@W and ISP@H measures.

Known-Groups Effects Summary

Known-groups	Effects on ISP@W			Effects on ISP@H				
	Det	Prev	D-P	TA	TP	TU	TS	TE
Gender		x	x	**X**		x	x	x
Education-level		x						
Education-level^		x	x					
G*E^*A^*Y^ Interaction	**X**		**X**					
University Area				x		x	x	
University Job-type			x					
Wkly. Hrs. of Business Computer Use								
Wkly. Hrs. of Home Computer Use		x	x	**X**	x	x	**X**	x
Wkly. Hrs. of Business Internet Use	x	x	**X**			x		
Wkly. Hrs. of Home Internet Use		x		**X**	x	x	**X**	x
Business Computer OS		x						
Home Computer OS						x		x
Business LAN Connection				**X**	x		x	**X**
Home LAN Connection				**X**	x		x	
Business Internet Connection	x				x			x
Home Internet Connection	x		x		x			
Business Computer Locations							x	

x – small effect | **X** – medium effect

Table 55

From Table 55, the 17 known-groups had 49 effects on security practice. ISP@W accounted for 18 effects (3 medium and 15 small). ISP@H accounted for 31 effects (8 medium and 23 small). A chi-square test between the number of medium versus small effects found no difference (X^2=.546, df=2, p<.46) between the known-groups effects on ISP@W and ISP@H.

The known-groups effects summary supported the following observations as answers to the fourth research question. 1) Education-level, education-level^, age^, years-of-computer-use^, and the G*E^*A^*Y^ interaction term had no effects on informal security practice. 2) University area known-groups had effects on informal security practice and no effects on formal security practice. 3) University job-type had no effects on informal security practice. 4) Business computer OS had no effects on informal security practice. Likewise, home computer OS had no effects on formal security practice. 5) Business LAN connection and home LAN connection had no effects on formal security practice. 6) Business computer locations had no effects on formal security practice.

Chapter Summary

The analysis of results presented in this chapter supported the literature review discussed in Chapter II and followed the methodology established in Chapter III. Findings from the content analysis, confirmatory factor analysis, SEM hybrid model analysis, and known-groups analysis answered the six research questions posed in Chapter II.

Outcome relative to the second research question included a measurement instrument. SEM results of assessing the instrument's content, construct validity, and reliability were presented in this chapter. Furthermore, confirmatory factor analysis and SEM hybrid model analysis outcome tested and retained the five research hypotheses posed in Chapter II. Moreover, the findings of this study supported the user-level ISA concept model posed in Chapter II. These results are a statistical profile or norms for future uses of the measurement instrument and future studies with respect to the user-level ISA concept.

CHAPTER V. CONCLUSIONS AND RECOMMENDATIONS

Introduction

This chapter summarizes the dissertation. The steps taken within the research study are reviewed, as well as discussions and conclusions about the research results. The chapter concludes with the research study's limitations, implications, and recommendations for future research.

Research Review

This study was undertaken in an effort to delineate user-level awareness and practice of information security among formal and informal computing-environments, as well as establish a foundation upon which to base further research. In particular, the following research questions were addressed:

RQ1. What is the domain of information security awareness?

RQ2. What are measures of information security awareness?

RQ3. Which information security practices reflect individual ISA?

RQ4. Do security practices differ between computing-environments?

RQ5. Does CSE influence individual ISA?

RQ6. Does PI influence individual ISA?

The methodology for this research followed the example of construct measurement detailed by Churchill (1979). Initially, qualifying the domain of ISA was specified through content analysis of the information security literature. This resulted in a definition of information security awareness and generated ISA characteristics of PI, CSE, individual ISA, ISP@W, and ISP@H. The relationships among these characteristics (refer to Chapter II, Figure 10) represented the user-level ISA concept within the ISA domain.

A measurement instrument was designed for the user-level ISA concept, which included known trait scales (PI and CSE), awareness measures (individual ISA), practice measures (ISP@W and ISP@H), demographic variables, and computing-environment technology variables. Using this instrument, data were collected through multiple iterations, including a face validity check (N=3), pre-test (N=7), pilot test (N=286), expert review (N=1), and a full-scale administration of the instrument (N=531). Undergraduate business students were a convenience sample for the pilot test and full-time Auburn University employees were a convenience sample for the full-scale instrument administration. Through the iteration process and data collected, the measurement instrument was refined. Also, the instrument reliability and validity were assessed. Lastly, the full-scale data were modeled and analyzed to provide a statistical profile of the user-level concept among full-time Auburn University employees.

The statistical profile serves as a norm for future use of the instrument. With respect to this study, the statistical profile also tested (p<.00) and retained the following hypothesis from the user-level ISA concept model (Figure 10).

H1: Higher measures of user-level ISA should positively affect user information security practice at work.

H2: Higher measures of user-level ISA should positively affect user information security practice at home.

H3: Information security practice at work, which have high measures of user-level ISA perspectives of policy and technology, should positively affect user information security practice at home.

H4: High measures of user-level PI should positively affect high measures of ISA.

H5: High measures of user-level CSE should positively affect high measures of ISA.

Discussions of the findings and conclusions from this research are presented in the next sections.

Discussion

Information security threats are dynamic, which require applicable countermeasures to protect the confidentiality, integrity, and availability of information. As a result, ISA has received varied attention in the information security literature as a training initiative. Also, numerous definitions of ISA existed in the literature with little empirical research. These definitions were not consensus and no study offered user-level ISA measurement techniques.

This research draws distinction between the user-level ISA concept (Figure 10) and ISA as training. The user-level ISA concept deals with measurement of individual user traits, security awareness, and security practices. Moreover, the user-level ISA concept identifies ISA sufficiency or insufficiency. In combination, the user-level ISA concept identifies and ISA training maintains security-positive behavior. The following examples reiterate the need to undertake this research project, which examined the awareness and practice of information security.

First, the literature (Schou and Trimmer, 2004) supported the user-level need for thorough comprehension of information security technologies. However, the most consistent comments received during the face-validity check and pre-test were potential lack of respondent comprehension in technology related terminology. An average 8.6% of full-time Auburn University employees (N=531) indicated a lack of comprehension for a particular survey question's terminology. The lack of user comprehension among particular survey questions ranged as high as 61% for technology hardware/software, 24% for individual ISA, 20% for ISP@W, and 28% for ISP@H. The survey instrument attributed a particular information security technology for each insufficiency.

Second, the literature (Lewis, Agarwal, and Sambamurthy, 2003) supported that individual beliefs about willingness to change (PI) and perceived technology capability (CSE) influenced information security technologies. CFA excluded personal innovativeness (PI) scale items that corresponded to late majority or laggard classifications (Hurt et al., 1977). Hence, the user-level ISA concept corresponded with concepts that classified users as innovators, early adopters, and early majority when perceiving the accomplishment of some future information security task.

Third, the literature (Straub, 1990; Kankanhalli, Teo, Tan, and Wei, 2003) noted that the formal, structured computer practices influencing effective information security where based on deterrence (policy) and/or control (technology). CFA of the user-level ISA concept supported this distinction and concurred with Kankanhalli et al. in that deterrent certainty efforts have greater influence than deterrent severity efforts. CFA excluded the *awareness of quarantining virus-infected computers* in lieu of the *awareness of virus protection software and updates*.

Fourth, a computer user could be anyone in a formal (i.e. structured) computing-environment or informal (i.e. unstructured) computing-environment. This differentiation presented an opportunity to identify information security obedience to formal policies (Thomson and von Solms, 2005) versus individual ISA. Within the user-level ISA concept, security practice comparisons (ISP@W versus ISP@H) filtered security practices influenced by information security obedience. Among ISP@W and ISP@H measures, information security obedience influenced five common practices. Formal security policies supported three practices, where each had high ISP@W frequency and low ISP@H frequency. CFA of the user-level ISA concept excluded these practices in both ISP@W and ISP@H. Also, two practices were contrary to formal security policies, where each had low ISP@W frequency and high ISP@H frequency. CFA of the user-level ISA concept retained these practices in ISP@H.

Lastly, users execute computer practices as rational choices, based on user-level perceptions of associated information security risks (Aytes and Connolly, 2004). Risky computer practice with perceived higher security risks were included in the survey instrument (7 ISP@W and 12 ISP@H). Also, six of the risky practice measures were common between computing-environments. CFA of the user-level ISA concept excluded five ISP@W and eight ISP@H higher risk measures, where each had low ISP@W frequency and low ISP@H frequency. Among the six retained risky measures; two were common measures to both computing-environments (*remotely connecting to computers to share drives, printers, or files* and *storing email locally rather than the email server*), one common practice was an exclusive measure of ISP@H (*allowing Web browsers to accept cookies from Web sites*), and one practice was a measure of ISP@H (*having other email accounts forwarded to one main email account*).

ISA Domain

The domain of ISA was addressed within this research by conducting a content analysis of the information security literature. This study developed the resulting definition, characteristics, and user-level ISA concept model, all of which specified the ISA domain.

The operational definition of ISA, as presented in Chapter IV, explained the ISA components without referencing the key terms of information, security, awareness, or practice. "Information" is manipulated data. Data is presented as numeric, text, graphic, image, video, or audio facts. "Security" is protection against threats. "Awareness" is having knowledge. Lastly, "Practice" is repetition to achieve improvement. These definitions also provide a statement about the purpose of ISA, namely the improvement in knowing computer data is protected from threats. The type of user-level improvement may be operational, tactical, or strategic. Consistency among research studies discussed in Chapter II supported these definitions.

Characteristics were collected among various reoccurring themes within the information security literature. Individual awareness (ISA) themes included learning style and computer literacy (demographic), appropriate hardware and software capabilities (technology), particular rules for acceptable behavior patterns (policy), and threat-to-countermeasure expertise (threat-context). Formal practice (ISP@W) themes included persuasion toward acceptable behavior patterns (deterrent efforts) and/or control within acceptable behavior pattern limits (preventive efforts). Informal practice (ISP@H) themes included appropriate threat-to-countermeasure application over information access points (access control, physical protection, user authentication, security management, and encryption). Lastly, human trait themes included individual beliefs about willingness to change (PI) and perceived technology capability (CSE). These ISA characteristics were delineated in Chapter II (Tables 8a, 8b, 8c, 9, 10, 11, and 12) as indicators to the extent of information security between formal and informal computing-environments.

Grouped in their respective themes, the developed ISA characteristics were also constructs of interest (PI, CSE, ISA, ISP@W, and ISP@H) that defined the user-level ISA concept, modeled in Chapter II (Figure 10). The user-level ISA concept provided the basis for developing a measurement instrument for ISA. Furthermore, this description of the ISA domain established a cornerstone for a common knowledge base.

ISA Measurement

The ISA measurement instrument developed in this research was the first attempt toward measuring the user-level ISA concept. The instrument was subject to multiple reviews and refinements prior to the full-scale administration. The reliability and validity of the instrument was demonstrated from the full-time Auburn University employee responses (N=531). The content and construct validity tests of the instrument facilitated greater internal and external validity (generalizability) of the measures (PI, CSE, ISA, ISP@W, and ISP@H). The thorough and systematic methodology employed in this research addressed survey design attributes from Grover, Lee, and Durand (1993) as well as Malhotra and Grover (1998), which assured that the development of quality ISA, ISP@W, and ISP@H measures employed sufficient rigor. Also, a statistical profile representing the current state of the user-level ISA concept among Auburn University employees was developed.

Known-groups among full-time Auburn University employee demographics indicated that the data provided through the survey sample were relevant for evaluating the instrument and establishing benchmarks of the user-level ISA concept. From the sample data, the distribution of responses among university areas (refer to Chapter IV, Table 18) and university job types (refer to Chapter IV, Table 19) were the same as in the Auburn University employee population. Appendix K noted that all of the employee respondents were computer users (N=531) in either a formal (n=493) and/or informal computing-environment (n=518). Also, over 90% of respondents reported more than 10 years of computer use (refer to Appendix K). These demographics supported Thomson and von Solms (1998) claim that computer users could be anyone in the organization.

The content validity of the instrument was established through the iterative process by which it was developed. The reliability of PI, CSE, individual ISA, ISP@W, and ISP@H measures was evaluated by computing Cronbach alpha coefficients among the construct measures for the pilot test (Table 16). Furthermore, construct reliability and factorial validity of the instrument were assessed via the information security awareness and practices of 531 computer users. The alpha coefficients for all five constructs were above the desired level of .8 (Nunnally, 1978). CFA of construct measures identified large-effect construct explanations among item-responses, where retained construct measures had equivalent or higher alpha coefficients. The retained construct measures were grouped into respective item subscales. The resulting 11 item subscales reported in Chapter IV (Tables 28 and 29) corresponded well with the characteristics determined from the content analysis of the literature. Among the nine item subscales with more than two measures, alpha coefficients were above .6, which was an acceptable cutoff for basic research studies (Nunnally, 1978).

The 11 item subscales or perspectives of the user-level ISA concept clearly divided into factors of awareness and practice. Three perspectives (technology, awareness, and threat-context) mapped directly to individual ISA. Three perspectives (deterrent efforts, deterrent-preventive efforts, and user authentication) mapped directly to ISP@W. Three other perspectives (access control, physical protection, and security management) mapped directly to ISP@H. Two common perspectives (preventive efforts and encryption) mapped to both ISP@W and ISP@H. The item subscales explained 52% of the variance between awareness and practices. Furthermore, the item subscales explained 57% of the variance between awareness, formal practice, and informal practice. Hence, the differentiation of computing-environment practice explained more employee response variation.

The measurement instrument developed in this study exhibited acceptable properties of validity and reliability. Content validity was established throughout the development process. Reliability was confirmed from the alpha coefficients of the constructs and item subscale measures. Factorial validity was demonstrated from factor analysis, where retained measures had large effect construct explanations and clustered around identifiable factors. Hence, this measurement instrument was deemed valid and reliable. The availability of this measuring instrument should facilitate further empirical research on information security and the user-level ISA concept.

ISA Practice

The results presented in Chapter IV identified ISA domain measures and differences between computing-environments. CFA, MR, and the SEM hybrid model analysis identified information security practices that reflected individual ISA. CFA identified individual awareness (Tables 25a, 25b, and 25c), formal practice (Tables 26a, 26b, and 26c) and informal practice (Tables 27a, 27b, 27c, 27d, and 27e) that were large-effect explanations of ISA domain measures. CFA also confirmed positive correlation among ISA domain measures within the user-level ISA concept (refer to Appendix H).

MR analysis of individual awareness, formal practice, and/or informal practice associations (Appendix I) identified unique measures (Table 32) within each respective construct. Individually, these unique measures explained other awareness or practice measures through large or medium effect relationships (Table 33). In combination, MR analysis identified awareness and unique practices that yielded individual security practice relationships with large and medium effect explanations (Tables 43 and 44). With respect to the user-level ISA concept, MR analysis identified that formal practice directly explained informal practice more than individual awareness.

The SEM hybrid model (Appendix J) represented the user-level ISA concept (refer to Chapter II, Figure 10) and depicted ISP@W as a mediator between individual ISA and ISP@H. The SEM results provided standardized direct, indirect, and total effects among ISA domain measures as support for the user-level ISA concept. SEM standardized direct effects (Appendix J and Table 38) identified individual ISA relationships between ISP@W and ISP@H (retained H1 and H2, respectively). SEM standardized indirect effects (Table 45) identified ISP@W as a moderator variable for individual ISA large-effect influence over informal practice ISA domain measures. SEM standardized total effects (Table 46) identified that individual ISA had stronger large-effect influence over informal practice (.94) than formal practice (.77). However, the formal practice construct was the stronger direct measure of individual ISA (.77 versus .33). Therefore, all formal and informal security practice reflected varying amounts of individual ISA.

Different computing-environments also yielded security practice differences among CFA, MR, hybrid model, and known-groups analysis. CFA inconsistently dropped and retained common security practice measures (W24 vs. H25 or W11 vs. H11), where the practice decision was made by an individual user (informal) rather than an individual user adhering to security policy (formal). Hence, policy contradictions were irrelevant and risky practice was more convenient in the absence of information security obedience. Informal technology awareness also differed, since the majority of respondents relied less on university supplied virus protection software.

MR analysis noted the disparity of individual awareness measures (policy, technology, and threat-context) among formal and informal security practice relationships. Policy awareness items (A06, A09, and A10) were included among informal relationship explanations (Table 43), yet deterrent-preventive items (W09 and W16) replaced policy awareness measures among the formal relationship explanations. Furthermore, stronger threat-context awareness explanations (82%) were found among formal practice explanations when compared to stronger technology awareness explanations (60%) found among informal practice explanations.

The hybrid model results (Appendix J) noted several security practice differences between computing-environments. Preventive efforts (technology awareness) explained more formal security practice variation and access control (threat-context awareness) explained more informal practice variation. Also, individual ISA had the stronger, direct influence on formal practice (retained H1) versus informal practice (retained H2). Formal security practice mediated the stronger ISA influence over a strong, direct influence (retained H3) on informal practice. Lastly, the user-level ISA concept explained 60% of the response variation among informal practice as compared to 7% of the formal practice. The informal practice measures, ordered by strength of explanation, were access control, encryption, security management, user authentication, and physical protection. Among these informal practice ISA domain measures, the top three informal practice measures were associated with security threat countermeasures (threat-context awareness) beyond the physical boundaries of the home environment.

Known-groups analysis provided several small or medium effect-size distinctions between environments (Table 55). Individual demographics influenced formal practice, while only gender influenced informal practice. University areas had effects on informal security practice whereas university job-type had effects on formal practice. Also, hours-of-use and hardware/software configurations between environments yielded more effects among informal practice (24) than formal practice (10).

Human Trait Influence on ISA

The literature review from Chapter II identified the human traits of PI and CSE as ISA domain measures within the user-level ISA concept. The results presented in Chapter IV supported that PI and CSE had influence on individual ISA and the user-level ISA concept. The following is a review of the results that supported PI and CSE influence on ISA.

The first iteration CFA identified and excluded the PI scale measures that were contrary to user-level ISA (refer to Chapter IV, Table 21). The second iteration CFA (Appendix H) identified that PI and CSE were positively correlated with individual ISA, ISP@W, and ISP@H. CFA results also concurred with Thatcher and Perrewé (2002) that PI correlated positively with CSE.

The user-level ISA concept (Figure 10) identified PI and CSE as direct influences on individual ISA. The SEM hybrid model (Appendix J) also represented the user-level ISA concept and tested individual ISA as a mediator of PI and CSE over ISP@W and ISP@H. The SEM results provided standardized direct, indirect, and total effects among ISA domain measures as support for PI and CSE influence and the mediating effect of individual ISA. SEM standardized direct effects (Appendix J and Table 38) identified PI and CSE had positive, direct relationships with individual ISA (retained H4 and H5, respectively). SEM standardized indirect effects (Table 45) identified individual ISA as a mediator for small-effect PI and CSE influence over formal and informal practice measures. SEM standardized total effects (Table 46) identified that PI had medium to small-effect influence while CSE had small-effect influence over ISA domain measures. PI had more influence than CSE for practice constructs and particular ISA domain measures. SEM hybrid model results (Appendix J) also identified that PI was positively correlated ($\rho \approx .14$, $p<.00$) with an unknown variable, outside of the user-level ISA concept, which explained the majority of formal practice response variation (93%). Therefore, all ISA domain measures reflect varying amounts of PI and CSE influence.

Known-groups analysis provided several small and one medium effect-size distinctions between PI and CSE (Tables 50, 51, 52, 53, and 54). Gender had small effects on both traits, yet individual demographics had medium effects on CSE. University areas had small effects on PI. Also, hours-of-use and hardware/software configurations between environments yielded small effects on PI (9) and CSE (8).

Statistical Profiles of the User-level ISA Concept

A statistical profile of the user-level ISA concept among Auburn University employees was computed from the measurement instrument and the results were presented in Chapter IV (Appendices F, G, and J). The overall means across the PI scales (11) and CSE scales (10) were 3.16 and 3.66 respectively, which fell on the five-point scale between an "average extent" and "a large extent" of individual beliefs. The overall means across individual ISA measures for technology (4), policy (3), and threat-context (9) were 3.85, 3.76, and 3.95 respectively, which were closer to "to a large extent" of awareness. Overall means across ISP@W measures for deterrent (1), preventive (6), and combined deterrent-preventive (4) efforts were 2.05, 2.09, and 2.25 respectively, which were closer to “to a small extent” of formal practice. Overall means across ISP@H measures for access control (6), physical protection (1), user authentication (2), security management (3), and encryption (3) were 2.29, 2.69, 2.15, 2.47, and 1.89 respectively, which also clustered around “a small extent” of informal practice. On average, 92% of the ISA domain measures were between “to a small extent” and “to a great extent” of the user-level ISA concept. In general, the ISA domain is present to some extent among full-time Auburn University employees.

The information from Chapter IV (Appendices F, G, and J) is presented, per Churchill’s (1979) recommendation, as a reference point for future uses of the user-level ISA concept developed in this research. Organizations that wish to assess the extent of user-level ISA concept may do so by applying the measurement instrument and determining how they relate to the benchmarks reported in these tables. Larger scores on an ISA domain measure would indicate a more extensive user-level ISA concept for that measure. Means and frequencies above those presented in Appendices F and G would indicate user-level ISA above the Auburn University employee norm, and conversely for means below the norm. The SEM hybrid model statistics from Appendix J may be used as research model norms in future studies that employ the measurement instrument (Appendix A) of the user-level ISA concept.

Conclusions

The overall conclusion is that the research questions posed in Chapter II were adequately addressed. Awareness and practice of information security were found to be qualified and quantified within the user-level ISA concept. The domain of ISA was delineated and operationalized as the extent of the user-level ISA concept among full-time Auburn University employees. Specific conclusions determined through this research are listed below.

1. The information security literature presented the need for a consensus level of understanding surrounding the awareness and practice of information security. This conclusion confirmed the need for the present study, which differentiated the user-level ISA concept from ISA training initiatives.

2. The domain of ISA was specified as distinct characteristics within a user-level conceptualization for the awareness and practice of information security. This operational definition of ISA was defined as *continuous deterrent and/or preventive efforts, which have the behavioral intent to limit the loss in data utility. These continuous efforts are derived and accomplished through the identification of possible threats, assessment of known risk or cost to loss ratio, and decision to mitigate the associated risk with employment of appropriate, associated threat-context countermeasures of access control, physical protection, user authentication, security management, and encryption.* The characteristics that constitute the operational definition of ISA were determined through a content analysis of the information security literature and corroborated by individual user's perceptions of information security awareness and security practice. The extent to which the user-level ISA concept is implemented was evidenced by the

degree to which the characteristics were realized by the individual computer user. The operational ISA definition and the user-level ISA concept, as determined through this research study, adequately specify the ISA domain.

3. Individual user's ISA domain characteristics are measurable by the instrument developed in this research. The measurement instrument was based on the user-level ISA concept, was operationalized in Appendix A, and Auburn University employee responses were modeled in Appendix J. The instrument is self-explanatory, convenient to computer users, and economical. The measurement instrument is self-explanatory in that it includes comprehensive instructions for completion by the respondent. The developed instrument is a Web-based questionnaire, which is convenient to computer users in that Internet connectivity, email, and an Internet browser are the minimum requirements for completion. As a Web-based questionnaire, the instrument is economical in respondent authentication, questionnaire delivery, and response collection. The instrument is also economical in that the respondent's time required for completion of the instrument in this study was approximately 20 minutes.

4. The measurement instrument developed in this study exhibited acceptable validity. The content validity of the instrument was established through multiple steps of the iterative process by which the instrument was developed. The multiple steps in the iterative process included multiple reviews by knowledgeable MIS faculty, experienced computer users, and practicing information security specialists. Factorial validity of the instrument was established through a factor analysis of individual information security awareness and information security practice data.

5. The measurement instrument exhibited acceptable reliability. The Cronbach alpha coefficients of construct measures were all above .8 for the pilot-test and full-scale administration. Also, alpha coefficients were above .6 for all the ISA domain measures.

6. A response to an item on the measurement instrument is directly interpretable. A user's response to the extent of an individual's belief, awareness, and practice of information security is over a five-point scale, ranging from "not at all" to "without question." For individuals who do not understand the concept of a particular awareness or practice question, the added response category of "I do not know" is available. Thus the degree of information security belief, awareness, or practice is reflected in the magnitude of the score for a particular item. As a reference for future use of this instrument, the mean scores of the ISA domain measures presented from the survey of full-time Auburn University employees is available in Appendix F.

7. The measurement instrument developed in this research study is representative of characteristics within the user-level ISA concept. Appendix J depicts the user-level ISA concept operationalized and modeled among information security beliefs, awareness, and practices of individual computer users. The user-level ISA concept determined that personal innovativeness (PI), computer self-efficacy (CSE), individual security awareness (ISA), security practice at work (ISP@W), and security practice at home (ISP@H) influence information security. Appendices F, G, H, and J also represent a statistical profile of the user-level ISA concept among full-time Auburn University employees. From this data, the user-level ISA concept was determined to exist to some extent.

8. Within the user-level ISA concept modeled in Appendix J, human traits of PI and CSE were determined to influence individual awareness of information security.

Individual ISA was determined to mediate PI and CSE influence among individual's practice of information security. The individual ISA mediation results are presented in Table 45.

9. Within the user-level ISA concept modeled in Appendix J, individual ISA was determined to influence both information security practice at work (ISP@W) and at home (ISP@H). Likewise, ISP@W was also determined to influence ISP@H. Furthermore, information security practice within the formal computing-environment (ISP@W) was determined to mediate individual ISA influence among individual's practice of information security within the informal computing-environment (ISP@H). The ISP@W mediation results are presented in Table 45.

Limitations of the User-level ISA Concept

The results and conclusions of this research study have limitations. The single method bias present in our lone survey instrument; the convenience sample of Auburn University employees; and the disturbance terms identified in the SEM hybrid model are study limitations, along with others that may have inadvertently been overlooked. Future research will address these issues. Future research will employ multiple methods to filter method bias. Future research will also sample multiple universities to approximate the university employee population. The disturbance terms identified in the SEM hybrid model from Appendix J will also be addressed in future research. In particularly, the disturbance term associated with information security practices in the formal computing environment (d2), which left 93% of the response variation among ISP@W unidentified.

Future research and further refinement of the user-level ISA concept will address the unexplained variance and lead to greater explanations and acceptance.

Implications of the User-level ISA Concept

The results and conclusions of this study have implications among practitioners and researchers alike. The user-level ISA concept represents the measurement of individual user's beliefs, awareness, and practice of information security. Moreover, the user-level ISA concept identifies user's ISA sufficiency or insufficiency. Also, the user-level ISA concept identifies user's ISA training needs, which are required to maintain security-positive behavior within computing-environments.

Guldentops (2002) noted top management's mission to ensure that IT objectives are met, IT risks are managed, and IT resources are used responsibly. As practitioners and owners of organizational information security, top management should employ the user-level ISA concept. The ISA domain characteristics among individual ISA and ISP@W are accommodating to information security technology and policy within the formal computing-environment. ISA domain measures among these characteristics are customizable to the individual organization, based on available technologies and particular policies. Also, top management should particularly note the relevance of PI, CSE, and individual ISA mediation across formal information security practice. Practice in the formal computing-environment directly influences security practice within the informal computing-environment, where work computing may be performed. Therefore, top management concerns over information risk associated with informal computing-environments should begin with formal security practice to minimize information risk associated with the formal computing-environment. Employment of the user-level ISA concept will identify ISA sufficiency and insufficiency. ISA training needs among users within the formal computing-environment should address insufficiencies and ISA sufficiency should address concerns of information risk.

The user-level concept of ISA and the developed measurement instrument is the first step toward a knowledge base for future research. Researchers should accept the challenge of opportunities presented by this information security research stream. The mediation of PI, CSE, and individual ISA offer additional branches for similar research efforts. Likewise, the refinement of ISA domain measures present similar research opportunities. As the results of this study were a response to a research call by Aytes and Connolly (2004), additional research should spawn from the recommendations for future research presented in this study.

Recommendations for Future Research

The results, conclusions, limitations, and implications of this study point to opportunities for additional research on the topic of awareness and practice of information security. Recommendations for future research are presented below.

1. The user-level ISA concept and resulting measurement instrument that were developed in this study should undergo further testing. Multiple studies, over multiple universities, that address further reliability and validity should lead to refinements and acceptance. University institutions were targeted in the initial research phase because relevant information security awareness concerns should be included in educational

programs, yet Siponen (2001) noted that this was seldom the case. Later in a similar process, specific industries would be targeted for in-depth analysis of the instrument.

2. Due to the disruptive nature of information technology, the user-level concept and measurement instrument should be incorporated in a longitudinal study to determine the extent of changes among awareness and practice of information security over time. Also, differences in ISA domain measures could be compared among industries, and between private and public sector organizations.

3. A particularly relevant area for future research is appraising the value of the user-level ISA concept. Heiser (2004) identified information security as an operational risk. Using the user-level ISA concept measure, studies should be initiated to relate the user-level ISA concept to other organizational factors. Determining how the user-level ISA concept relates to organizational effectiveness would be a relevant study. Given the reluctance of top management to embrace information security, results that verify or refute the value of information security would be especially relevant. The user-level ISA concept and measurement instrument developed in the present study provides the means to accomplish such research.

Chapter Summary

The purpose of this research was to develop a better understanding of the awareness and practice of information security, and that goal was achieved. The results of this dissertation include a delineation of the ISA domain, a tested instrument for measuring the extent of user-level ISA, a tested model of the user-level ISA concept, and a statistical profile of user-level ISA among full-time employees of a public research university.

This research was conceived with the intent to be a foundation upon which to base further work. Hence, this study should be viewed as the first step in a comprehensive research program to study the awareness and practice of information security. Furthermore, the cornerstone was set for further empirical study and several research initiatives were proposed earlier in this chapter. Moreover, the study's results serve as a tool for information security practitioners and as a guide for curriculum development by academics.

Aytes and Connolly (2004) called for the development of a research model that concentrated on factors most directly related to user's acceptance of countermeasures and incorporated user's perceptions and decision-making processes to improve information security. The results from this study provide a response to this call, with the user-level ISA concept model and measurement instrument to test user's awareness and practice of information security.

REFERENCES

Adams, D. A.; Nelson, R. R.; and Todd, P. A. (June, 1992). Perceived usefulness, ease of use, and usage of information technology: A replication. *MIS Quarterly*, 16(2), pages 227 – 247.

Allen, M. J. and Yen, W. M. (1979). *Introduction to Measurement Theory*. Monterey, California: Brooks-Cole.

Amarasinghe, S. (2004). Endpoint intrusion prevention—seven criteria for success. Online http://www.determina.com/docs/EndpointIntrusionPrevention-SevenCriteria.pdf, pages 1-9, accessed 3/21/ 2005.

Andreu, R.; Ricart, J. E.; and Valor, J. (1994). Information systems planning at the corporate level. In Ciborra, C. and Jelassi, T. (eds.), *Strategic Information Systems: A European Perspective*. Chichester, UK: John Wiley and Sons, pages 23 – 52.

Auburn University. (2006a). Office of Information Technology: Information Technology Policies for Auburn University. Online http://www.auburn.edu/oit/it_policies/index.php, pages 1-17, accessed 1/09/ 2006.

Auburn University. (2006b). Office of Information Technology: Hardware and Software for Auburn University. Online http://www.auburn.edu/oit/hardware_software, pages 1-11, accessed 1/09/ 2006.

Aytes, K. and Connolly, T. (September, 2004). Computer Security and risky computing practices: A rational choice perspective. *Journal of Organizational and End User Computing*, 16(3), pages 22 – 40.

Ball, L. and Harris, R. (March, 1982). SMIS members: A membership analysis. *MIS Quarterly*, 6(1), pages 19 – 38.

Banavar, G. and Bernstein, A. (2004). Challenges in design and software infrastructure for ubiquitous computing applications. *Advances in computers*, 62, pages 179 – 202.

Bandura, A. (April, 1977). Self-efficacy: Toward a unifying theory of behavioral change. *Psychological Review*, 84(2), pages 191 – 215.

Bandura, A. (1986). *Social foundations of thought and action—a social cognitive theory*. Englewood Cliffs, New Jersey: Prentice-Hall.

Baptista, R. (February, 1999). The diffusion of process innovations: A selective review. *International Journal of the Economics of Business*, 6(1), pages 107 – 129.

Bartoli, A.; Hermel, P.; and Ramis-Pujol J., (June, 2003). Innovation assessment as a management information tool: a case study. *Measuring Business Excellence*, 7(2), pages 6-20.

Bernstein, I. H. (1988). *Applied Multivariate Analysis*. New York: Springer-Verlag.

Bigoness, W. J. and Perreault, W. D. (March, 1981). A conceptual paradigm and approach for the study of innovators. *Academy of Management Journal*, 24(1), pages 68 – 82.

Bollen, K. A. (1989). *Structural Equations With Latent Variables*. New York: John Wiley & Sons.

Bommer, M. and Jalajas, D. S. (January,1999). The threat of organizational downsizing on the innovative propensity of R&D professionals. *R&D Management*, 29(1), pages 27 – 34.

Boockholdt, J. L. (June, 1989). Implementing security and integrity in micro-mainframe networks. *MIS Quarterly*, 13(2), pages 135 – 144.

Brancheau, J. C. and Wetherbe, J. C. (March, 1987). Key issues in information systems management. *MIS Quarterly*, 11(1), pages 23 – 45.

Brancheau, J. C.; Janz, B. D.; and Wetherbe, J. C. (June, 1996). Key issues in information systems management: 1994-95 SIM Delphi results. *MIS Quarterly*, 20(2), pages 225 – 242.

Bratton, G. R. and Newsted, P. R. (September, 1995). Response effects and computer-administered questionnaires: The role of the entry task and previous computer experience. *Behaviour and Information Technology*, 14(5), pages 300 – 312.

Breidenbach, S. (August, 2000). How secure are you? *InformationWeek*, issue 800, pages 71 – 75.

Brenner, W. (January, 2005). A license to browse? Online via searchsecurity.com http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci1035299,00.html, pages 1 – 4, accessed 3/21/2005.

Brios, D. P.; George, J. F.; and Zmud, R. W. (June, 2002). Inducing sensitivity to deception in order to improve decision making performance: A field study. *MIS Quarterly*, 26(2), pages 119 – 144.

Brown, C. V. and Magill, S. L. (December, 1994). Alignment of the IS functions with the enterprise: Toward a model of antecedents. *MIS Quarterly*, 18(4), pages 371 – 403.

Brown, A. E. and Grant, G. G. (May, 2005). Framing the frameworks: A review of IT governance research. *Communications of the Association for Information Systems*, 15, pages 696 – 712.

Budd, R.; Thorp, R.; and Donohew, L. (1967). *Content Analysis of Communications*. New York: Macmillian Company.

Byrne, B. M. (2001). *Structural Equation Modeling with AMOS: Basic Concepts, Applications, and Programming*. Mahwah, New Jersey: Lawrence Erlbaum Associates, Incorporated.

Carmines, E. G. and Zeller, R. A. (1979). *Reliability and validity assessment*. Newbury Park, California: Sage Publications.

Carney, T. F. (1972). *Content Analysis*. London: B. T. Batsford Limited

Carr, H. H. and Snyder, C. A. (2004). *Network Security*. Anderson, South Carolina: Tavenner Publishing Company.

Chapple, M. (December, 2003). What constitutes acceptable use? Online http://searchsecurity.techtarget.com/tip/1,289483,sid14_gci940236,00.html, pages 1 – 2, accessed 3/21/2005.

Chau, P. Y. K. (Fall, 1996). An empirical assessment of a modified technology acceptance model. *Journal of Management Information Systems*, 13(2), pages 185 – 204.

Chin, W. W. and Todd, P. A. (June, 1995). On the use, usefulness, and ease of use of structural equation modeling in MIS research: A note of caution. *MIS Quarterly*, 19(2), pages 237 – 246.

Churchill, G. A. (February, 1979). A paradigm for developing better measures of marketing constructs. *Journal of Marketing Research*, 16(1), pages 64 – 73.

Claburn, T. (February, 2005). Security chiefs sit high on the corporate ladder. *InformationWeek*, issue 1028, pages 59 – 61.

Cline M., and Jensen, B. K. (August, 2004). Information security: An organizational change perspective. *Proceedings of the Tenth Americas Conference on Information Systems*. New York, New York.

Cohen, J. (1977). *Statistical Power Analysis for the Behavioral Sciences*, (Revised Edition). New York: Academic Press, Incorporated.

Compeau, D. R. and Higgins, C. A. (June, 1995). Computer self-efficacy: Development of a measure and initial test. *MIS Quarterly*, 19(2), pages 189 – 211.

Creswell, J. W. (1994). *Research design: Qualitative and quantitative approaches*. Thousand Oaks, California: Sage Publications, Incorporated.

Cronbach, L. J. (1971). Test validation. In Thorndike, R. L. (ed.) *Educational Measurement* (Second Edition). Washington, DC: American Council on Education, pages 443 – 507.

Cronbach, L. J. and Meehl, P. E. (1955). Construct validity in psychological tests. *Psychological Bulletin*, 52, pages 281 – 302.

D'Antoni, H. (October, 2001). Hacker hires don’t interest most businesses. *InformationWeek*, issue 860, pages 93 – 94.

D'Antoni, H. (July, 2002). Security breaches know no boundaries. *InformationWeek*, issue 896, page 46.

Davis, F. D. (September, 1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, 13(3), pages 319 – 340.

Deloitte Touche Tohmatsu International (August, 2005). 2005 Global Security Survey Financial Services Industry Results. *Computer Security Update*, 6(8). Online http://proquest.umi.com/pqdlink?did=870269431&sid=1&Fmt=3&clientId=1997&RQT=309&VName=PQD, pages 1 – 4, accessed 3/20/2006.

Diamond, S. (August, 1995). Client/server: Myths and realities. *Journal of Systems Management*, 46(4), pages 44 – 48.

Dickson, G. W.; Leitheiser, R. L.; Wetherbe, J. C.; and Nechis, M. (September, 1984). Key information systems issues for the 1980's. *MIS Quarterly*, 8(3), pages 135 – 159.

Dixon, N. M. (August, 1998). The responsibilities of members in an organization that is learning. *The Learning Organization*, 5(4), pages 161 – 167.

Dunn, T. S. (1982). *Methodology for the optimization of resources in the detection of computer fraud.* Unpublished doctoral dissertation, University of Arizona, Arizona.

Egan, M. (December, 2004). *The 10 traits of effective security*. Online http://searchnetworking.techtarget.com/tip/1,289483,sid7_gci1033304,00.html, pages 1 – 3, accessed 3/21/05.

Egan, M. and Mather, M. C. (2004). *The executive guide to information security: Threats, challenges, and solutions*. Boston, Massachusetts: Addison-Wesley Professional.

Ferrarini, E. M. (2001). *The five-access point security plan*. Online http://www.enterprisenetworkingplanet.com/netsecur/article.php/752421, pages 1 – 4, accessed 3/20/2005.

Fichman, R. G. and Kemerer, C. F. (September, 1999). The illusory diffusion of innovation: An examination of assimilation gaps. *Information Systems Research*, 10(3), pages 255 – 275.

Fitzgerald, K. J. (1995). Information security baselines. *Information Management & Computer Security*, 3(2), pages 8 – 12.

Fishbein, M. and Ajzen, I. (1975). *Belief, attitude, intention, and behavior: An introduction to theory and research*. Reading, Massachusetts: Addison-Wesley Publishing.

Fowler, D. (1999). *Virtual private networks: Making the right connection*. San Francisco: Morgan Kaufmann Publishers, Incorporated.

Forcht, K. A. (1994). *Computer security management*. Danvers, Massachusetts: Boyd and Fraser Publishing.

Frank, K. A. and Fahrbach, K. (May, 1999). Organization culture as a complex system: Balance and information in models of influence and selection. *Organization Science*, 10(3), pages 253 – 277.

Franklin, C. (December, 2004). Survivor's guide to 2005: Security. *Network Computing*, 15(26), pages 20 – 29.

Franklin, C. (February, 2005). Market Analysis: Strong authentication. *Network Computing*, 16(2), pages 34 – 51.

Friedkin, N. E. and Cook, K. S. (August, 1990). Peer group influence. *Sociological Methods and Research*, 19(1), pages 122 – 143.

Friedman, A. and Cornford, D. (1989). *Computer System Development: History, Organization, and Implementation*. Chichester, England: John-Wiley and Sons.

Furnell, S. M; Gennato, M.; and Dowland, P. S. (September, 2002). A prototype tool for information security awareness and training. *Logistics Information Management*, 15(5/6), pages 352 – 357.

Gattiker, U. E. and Kelley, H. (September, 1999). Morality and computers: Attitudes and differences in moral judgments. *Information Systems Research*, 10(3), pages 233 – 254.

Gist, M. E and Mitchell, T. R. (April, 1992). Self-efficacy: A theoretical analysis of its determinants and malleability. *Academy of Management Review*, 17(2), pages 183 – 211.

Green, M. C. and Brock, T. C. (February, 2005). Organizational membership versus informal interaction: Contributions to skills and perceptions that build social capital. *Political Psychology*, 26(1), pages 1 – 25.

Grover, V. (1993). An empirically derived model for the adoption of customer-based interorganizational systems. *Decision Sciences*, 24(3), pages 603 – 639.

Grover, V.; Lee, C. C.; and Durand, D. (June, 1993). Analyzing methodological rigor of MIS survey research from 1980–1989. *Information and Management*, 24(6), pages 305 – 317.

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

Gouldner, A. W. (1954). *Patterns of Industrial Bureaucracy*. New York: Free Press.

Guldentops, E. (2002). Governing information technology through COBIT. In Gertz, M.; Guldentops, E.; and Strous, L. (eds.), *Integrity, Internal Control and Security in Information Systems: Connecting governance and technology*. Norwell, Massachusetts: Kluwer Academic Publishers, pages 115 - 133.

Gupta, M.; Rao, R.; and Upadhyaya, S. (September, 2004). Electronic banking and information assurance issues: Survey and synthesis. *Journal of Organizational and End User Computing*, 16(3), pages 1 – 21.

Hair Jr., J. F.; Anderson, R. E.; Tatham, R. L; and Black, W. C. (1995). *Multivariate Data Analysis with Readings*, (Fourth Edition). Prentice Hall: Englewood Cliffs, New Jersey.

Hannemyr, G. (2003). The Internet as hyperbole. Online http://heim.ifi.uio.no/~gisle/essay/diff.html, 18 pages, accessed 6/9/2005.

Harman, H. H. (1976). *Modern Factor Analysis*, Chicago: University of Chicago Press.

Harrington, S. J. (September, 1996). The effect of codes of ethics and personal denial of responsibility on computer abuse judgments and intentions. *MIS Quarterly*, 20(3), pages 257 – 278.

Harris, S. G. (June, 1994). Organizational culture and individual sense making: A schema-based perspective. *Organization Science*, 5(3), pages 309 – 321.

Harrison, A. W. and Rainer, Jr., R. K. (Summer, 1992). The influence of individual differences on skill in end-user computing. *Journal of Management Information Systems*, 9(1), pages 93 – 111.

Hawkins, S.; Yen, D. C.; and Chou, D. C. (2000). Awareness and challenges of Internet Security. *Information Management & Computer Security*, 8(3), pages 131 – 143.

Heiser, J. G. (July, 2004). The regulation of information security. *Intermedia*, 32(2), pages 29 – 30.

Hofstede, G. (1984). *Cultures Consequences: International Differences in Work-Related Values*. Beverly Hills, CA: Sage Publications.

Horton, Jr., F. W. (1985). *Information resources management: Harnessing information assets for productivity gains in the office, factory, and laboratory*. Englewood Cliffs, New Jersey: Prentice Hall.

Hsaio, D. K.; Kerr, D. S.; and Madnick, S. F. (1979). *Computer Security*, New York: Academic Press.

Huff, S. L. and Monroe, M. C. (December, 1985). Information technology assessment and adoption: A field study. *MIS Quarterly*, 9(4), pages 327 – 340.

Hulme, G. V. (January, 2005). Another fight to wage. *InformationWeek*, issue 1022, pages 60 – 63.

Hulme, G. V. (September, 2004). Hercules bulks up security. *InformationWeek*, issue 1005, page 63.

Hulme, G. V. (August, 2002). Virus defenses reach the tipping point. *InformationWeek*, issue 901, page 56.

Hulme, G. V. (July, 2002). Guarded optimism. *InformationWeek*, issue 896, pages 36 – 50.

Hulme, G. V. (September, 2001a). Management takes notice. *InformationWeek*, issue 853, pages 28 – 34.

Hulme, G. V. (September, 2001b). Security policies: How much is enough? *InformationWeek*, issue 853, pages 74 – 75.

Hulme, G. V. (October, 2000). Beware of the threat from within. *InformationWeek*, issue 808, pages 235 – 238.

Hurt, H. T.; Joseph, K.; and Cook, C. D. (Fall, 1977). Scales for the measurement of innovativeness. *Human Communication Research*, 4(1), pages 58 – 65.

Huston, T. (September, 2001). Security issues for implementation of e-medical records. *Communications of the ACM*, 44(9), pages 89 – 94.

Information Systems Security Association (December, 2003). 2003 ISSA/BSA Security Survey Results. Online via http://www.issa.org/PDF/research-BSA-ISSA.pdf , pages 1 - 23, accessed 5/19/2005.

Information Systems Security Association (January, 2005). 2004 ISSA/BSA Security Survey Results. Online via http://www.issa.org/PDF/BSA_ISSA_full.ppt, pages 1 - 44, accessed 5/19/2005.

Irvine, C. E. and Levin, T. E. (2002). A cautionary note regarding the data integrity capacity of certain secure systems. In Gertz, M.; Guldentops, E.; and Strous, L. (eds.), *Integrity, Internal Control and Security in Information Systems: Connecting governance and technology*. Norwell, Massachusetts: Kluwer Academic Publishers, pages 3 - 25.

Jackall, R. (1988). *Moral Mazes: The World of Corporate Managers*. New York: Oxford University Press.

Kachigan, S. K. (1982). *Multivariate statistical analysis*. New York: Radius Press.

Kahin, B. and Keller, J. H. (eds.) (1997). *Coordinating the Internet*. Cambridge, Massachusetts: The MIT Press.

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

Kanter, R. M. (2003). Introduction: Getting the Best from Best Practices. *In Best Practice: Ideas and Insights from the World's Foremost Business Thinkers*. Cambridge, Massachusetts: Perseus Publishing.

Kearvell-White, B. (1996). National (UK) computer security survey 1996. *Information Management & Computer Security*, 4(3), pages 3 – 17.

Kegerreis, R. J.; Engel, J. F.; and Blackwell, R. D. (1970). Innovativeness and Diffusiveness: A marketing view of the characteristics of earliest adopters. In Kollat, D. T., Blackwell, R. D., and Engel, J. F. (eds.), *Research in consumer behavior*. New York: Holt, Rinehart and Winston, pages 671 – 689.

Keizer, G. (February, 2005). Spam could cost businesses worldwide $50 billion. *InformationWeek*, issue 1028, page 18.

Khazanchi, D. and Sutton, S. G. (January, 2001). Assurance services for business-to-business electronic commerce: A framework and implications. *Journal of the Association of Information Systems*, 1(11), pages 1 – 53.

Kim, J. O. and Mueller, C. W. (1982). *Introduction to factor analysis*. Beverly Hills: Sage Press.

Kiesler, S. and Sproull, L. S. (Fall, 1986). Response effects in the electronic survey. *Public Opinion Quarterly*, 50(3), pages 402 – 413.

King, W.R. (1988, October). How effective is your information systems planning? *Long Range Planning*, 21(5), pages 103-112.

Kline, R. B. (1998). *Principles and Practice of Structural Equation Modeling*. NewYork: The Guliford Press.

Klerlinger, F. (1986). *Foundations of Behavioral Research* (Third Edition). New York: Holt, Rinehart, and Winston.

Klete, H. (1978). Some minimum requirements for legal sanctioning systems special emphasis on detection. In Blumstein, A.; Cohen, J.; and Nagin, D. (eds.), *Deterrence and incapacitation: Estimating the effects of criminal sanctions on crime rates*. Washington, D.C.: National Academy of Sciences.

Knapp, K.; Morris, F.; Rainer, R. K.; and Byrd, T.A. (December, 2003). Defense mechanisms of biological cells: A framework for network security thinking. *Communications of the Association for Information Systems*, 12, pages 701-719.

Kotullic, A. G. and Clark, J. G. (May, 2004). Why there aren't more information security research studies. *Information & Management*, 41(5), pages 597-607.

Kraemer, K. L. and Dutton, W. H. (1991). Survey research in the study of management information systems. In Kraemer, K. L. (ed.), *The Information systems research challenge: Survey research methods*, Volume 3. Boston, Massachusetts: Harvard Business School, pages 3 - 26.

Kruger, H. A. and Kearney, W. D. (June, 2006). A prototype for assessing information security awareness. *Computers & Security*, 25(4), pages 1 – 8.

Larson, A. K. (July, 1999). Global security survey virus attack. *InformationWeek*, issue 723, pages 42 – 56.

Lamb, R. and Kling, R. (June, 2003). Reconceptualizing users as social actors. *MIS Quarterly*, 27(2), pages 197 – 235.

Lasswell, H. D. (1977). Building as political communication: The signature of power on environment. In Lerner, D. and Nelson, L. M. (eds.), *Communication Research—a Half-Century Appraisal*. Honolulu: The University Press of Hawaii, pages 280 – 294.

Lawshe, C. H. (Winter, 1975). A quantitative approach to content validity. *Personnel Psychology*, 28(4), pages 563 – 575.

Leach, J. (December, 2003). Improving user security behavior. *Computers and Security*, 22(8), pages 685 – 692.

Lederer, A. L. and Sethi, V. (Winter, 1992). Root causes of strategic information systems planning implementation problems. *Journal of Management Information Systems*, 9(1), pages 25 – 45.

Lee, W. (2003). *Windows XP Unwired*. Sebastopol, California: O'Reilly & Associates, Incorporated.

Lewis, B. R. (1993). *The information resource management concept: Domain, measurement, and implementation status.* Unpublished doctoral dissertation, Auburn University, Alabama.

Lewis, B. R.; Snyder, C. A.; and Rainer, Jr., R. K. (Winter, 1995). An empirical assessment of the information resource management construct. *Journal of Management Information Systems*, 12(1), pages 199 – 223.

Lewis, W.; Agarwal, R.; and Sambamurthy, V. (December, 2003). Sources of influence on beliefs about information technology use: An empirical study of knowledge workers. *MIS Quarterly*, 27(4), pages 657 – 678.

Lipschutz, R. P.; Steinhart, M. J.; and Gambhir, S. (June, 2004). Business security. *PC Magazine*, 23(11), pages 130 – 136.

Loch, K. D.; Carr, H. H.; and Warkentin, M. E. (June, 1992). Threats to information systems: Today's reality, yesterday's understanding. *MIS Quarterly*, 16(9), pages 173 – 186.

Loeber, M. (August, 2004). Exactly what is a Sarbanes-Oxley anyhow? Online http://search400.techtarget.com/tip/1,289483,sid3_gci1001949,00.html, accessed 3/21/05.

Lord, R. G.; De Vader, C. L.; and Alliger, G. M. (August, 1986). A meta-analysis of the relation between personality traits and leadership perceptions: An application of validity generalization procedures. *Journal of Applied Psychology*, 71(3), pages 402 – 410.

Lyytinen, K. and Rose, G. M. (December, 2003). The disruptive nature of information technology innovations: The case of Internet computing in systems development organizations. *MIS Quarterly*, 27(4), pages 557 – 595.

Ma, Q. and Pearson, J. M. (April, 2005). ISO 17799: "Best Practices" in information security management? *Communications of the Association for Information Systems*, 15, pages 577 – 591.

Mack, M. (December, 2004). Market analysis: CSI—Enterprise. *Network Computing*, 15(25), pages 32 – 53.

Madnick, S. (1978). Management policies and procedures needed for effective computer security. *Sloan Management Review*, 20(1), pages 61 – 74.

Madnick, S. E. and Wang, R. Y. (Fall, 1988). Evolution towards strategic applications of databases through composite information systems. *Journal of Management Information Systems*, 5(2), pages 5 – 22.

Malhotra, M. K. and Grover, V. (July, 1998). An assessment of survey research in POM: From constructs to theory. *Journal of Operations Management*, 16(4), pages 407 – 425.

March, J. G. and Olsen, J. P. (1989). *Rediscovering Institutions: The Organizational Basis of Politics*. New York: Free Press.

Marcoulides, G. A. and Hershberger, S. L. (1997). *Multivariate Statistical Methods: A First Course*. Mahwah, New Jersery: Lawrence Erlbaum Associates, Incorporated.

Marks, S. J. (January, 2005). Computer gatekeepers. *ColoradoBiz*, 32(1), pages 48 – 51.

Martin, J. (1973). *Security, accuracy, and privacy in computer systems*. Englewood Cliffs, New Jersey: Prentice-Hall Publishing, Incorporated.

McAdam, R. (December, 2000). Knowledge management as a catalyst for innovations within organizations: A qualitative study. *Knowledge and Process Management*, 7(4), pages 233 – 241.

McFarlan, F. W. and McKenney, J. L. (September, 1982). The information archipelago—gaps and bridges. *Harvard Business Review*, 60(5), pages 109 – 119.

McFarlan, F. W.; McKenney, J. L.; and Plyburn, P. (January, 1983). The information archipelago—plotting a course. *Harvard Business Review*, 61(1), pages 145 – 156.

McFarlan, F. W. and McKenney, J. L. (1983). *Corporate information systems: The issues facing senior executives*. Homewood, Illinois: Richard D. Irwin, Incorporated.

Mendelson, E.; Randall, N.; Schenk, R.; Janowski, D. D.; and Garcia, A. R. (December, 2000). The danger within. *PC Magazine*, 19(21), pages 203 – 213.

Molta, D. and Bulk, F. (February, 2005). WLANs bust out. *Network Computing*, 16(30), pages 37 – 64.

Morgan, A. and Chen, C. (August, 2003). Integrity, internal control and security in information systems: Connecting governance and technology. *Journal of the American Society for Information Science and Technology*, 54(10), page 976.

Murphy, C. (July, 2002). IT security reaches the top. *InformationWeek*, issue 896, page 50.

Nance, W. D. and Straub, D. W. (1988). An investigation into the use and usefulness of security software in detecting computer abuse. *Proceedings of the ninth annual International Conference on Information Systems*, pages 283 – 294. Minneapolis, Minnesota.

National Computing Centre (1998). The Business Information Security Survey 1998 (BISS 1998) – Information Security, the True Cost to Business. Online http://www.ncc.co.uk/ncc/biss1998.pdf, pages 1-12, accessed 3/21/ 2005.

National Computing Centre (2000). The Business Information Security Survey 2000 (BISS 2000). Online http://www.ncc.co.uk/ncc/biss2000.pdf, pages 1-10, accessed 3/21/ 2005.

Nayar, M. K. (2002). The information integrity imperative. In Gertz, M.; Guldentops, E.; and Strous, L. (eds.), *Integrity, Internal Control and Security in Information Systems: Connecting governance and technology*. Norwell, Massachusetts: Kluwer Academic Publishers, pages 187 - 193.

Nelson, D. L. (1990). Individual adjustment to information-driven technologies: A critical review. *MIS Quarterly*, 14(1), pages 87 – 98.

Niederman, F.; Brancheau, J. C.; and Wetherbe, J. C. (December, 1991). Information systems management issues for the 1990s. *MIS Quarterly*, 15(4), pages 475 – 500.

Nunnally, J. C. (1967). *Psychometric Theory*. New York: McGraw-Hill.

Nunnally, J. C. (1978). *Psychometric Theory* (Second Edition). New York: McGraw-Hill.

Ocasio, W. (June, 1999). Institutionalized action and corporate governance: The reliance on rules of CEO succession. *Administrative Science Quarterly*, 44(2), pages 384 – 416.

Parker, D. B. (1981). *Computer security management*. Reston, Virginia: Reston Publishing.

Parker, D. B. (1983). *Fighting computer crime*. New York: Scribner Publishing.

Pinsonneault, A. and Kraemer, K. L. (Spring, 1993). Survey research methodology in management information systems: An assessment. *Journal of Management Information Systems*, 10(2), 75-105.

Rajagopalan, N. and Spreitzer, G. (January, 1997), Toward a theory of strategic change: A multi-lens perspective and integrative framework, *The Academy of Management Review*, 22(1), 48-79.

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

Rainer, Jr., R. K. and Harrison, A. W. (1993). Toward development of the end user computing construct in a university setting. *Decision Sciences*, 24(6), pages 1187 – 1202.

Rainer, Jr., R. K.; Snyder, C. A.; and Carr, H. H. (September, 1989). Risk analysis for information technology. *Journal of Management Information Systems*, 8(1), pages 129 – 147.

Ramanathan, R. R. (December, 2004). Information security top-down. *Security*, 41(12), pages 30 – 34.

Riech, B. H. and Benbasat, I. (March, 2000). Factors that influence the social dimension of alignment between business and information technology objectives. *MIS Quarterly*, 24(1), pages 82 – 113.

Roberts, P. (November, 2004). Big picture security. *InfoWorld*, 44, pages 36 – 50.

Rogers, E. M. (1995). *Diffusion of Innovations* (Fourth Edition). New York: The Free Press.

Ross, J. W. (March, 2003). Creating a strategic IT architecture competency: Learning in stages. *MIS Quarterly Executive*, 2(1), pages 31 – 43.

Ross, R.; Katzke, S.; Johnson, A.; Swanson, M.; Stoneburner, G.; Rogers, G.; and Lee, A. (February, 2005). Recommended security controls for federal information systems. *NIST Special Publication 800-53*, National Institute of Standards and Technology, U.S. Department of Commerce, Washington DC: U.S. Government Printing Office.

Ryan, S. D. and Bordoloi, B. (March, 1997). Evaluating security threats in mainframe and client/server environments. *Information & Management*, 32(3), pages 137 – 146.

Sambamurthy, V. and Zmud, R. W. (June, 1999). Arrangements for information technology governance: A theory of multiple contingencies. *MIS Quarterly*, 23(2), pages 261 – 290.

Sanders, A. D. (January, 2003). Utilizing simple hacking techniques to teach system security and hacker identification. *Journal of Information Systems Education*, 14(1), pages 5 – 9.

Sarkar, D. (December, 2004). Two converging worlds: Cyber and physical security. *Federal Computer Week*, 18(42), pages 56 – 57.

Schein, E. H. (1999). *The Corporate Culture Survival Guide*. San Francisco, California: Jossey-Bass Publishers.

Schein, E. H. (1985). *Organizational Culture and Leadership: A Dynamic View*. San Francisco, California: Jossey-Bass Publishers.

Schlarman, S. (March, 2002). The case for a security information system. *Information Systems Security*, 11(1), pages 44 – 50.

Schneier, B. (2000). *Secrets and Lies: Digital security in a networked world*. Indianapolis, Indiana: Wiley Publishing, Incorporated.

Schou, C. D. and Trimmer, K. J. (September, 2004). Information assurance and security. *Journal of Organizational and End User Computing*, 16(3), pages i – vii.

Schultz, K. (October, 2004). Spyware exterminators. *InfoWorld*, 40, pages 43 – 47.

Schumpeter, J. (1934). *The Theory of Economic Development*. Boston, Massachusetts: Harvard University Press.

Schwartz, M. (December, 2004). Security on a shoestring: Creating internet policies on the cheap. Online http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci1037425,00.html via searchsecurity.com, pages 1 – 3, accessed 3/21/2005.

Scott, J. E. (April, 2004). Measuring dimensions of perceived e-business risks. *Information Systems and eBusiness Management*, 2(1), pages 31 – 55.

Sethi, V. and King, W. R. (July, 1991). Construct measurement in information systems research: An illustration in strategic systems. *Decision Sciences*, 22(4), pages 455 – 472.

Sethi, V. and King, W. R. (December, 1994). Development of measures to assess the extent to which an information technology application provides competitive advantage. *Management Science*, 40(12), pages 1601 – 1627.

Shanks, J. M. (1991). Computer-assisted surveys: Recent progress and future developments. In Kraemer, K. L. (ed.), *The Information systems research challenge: Survey research methods*, Volume 3. Boston, Massachusetts: Harvard Business School, pages 211 - 234.

Sherman, E. (May, 2004). Prove it. *Information Security*, 7(5), pages 24 – 29.

Silver, M. S., Markus, M. L., and Beath, C. M. (September, 1995). The information technology interaction model: A foundation for the MBA core course. *MIS Quarterly*, 19(3), 361-391.

Siponen, M. T. (January, 2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security*, 8(1), pages 31 – 41.

Siponen, M. T. (June, 2001). Five dimensions of information security awareness. *Computers and Society*, 31(2), pages 24 – 29.

Smith, S. L. (1987). Authenticating users by word association. *Computers and Security*, 6(0), pages 464 – 470.

Spurling, P. (March, 1995). Promoting security awareness and commitment: Alcoa encourages people to be honest. *Information Management & Computer Security*, 3(2), pages 20 – 26.

Stahl, B. C. (September, 2004). Responsibility for information assurance and privacy: A problem of individual ethics? *Journal of Organizational and End User Computing*, 16(3), pages 59 – 77.

Stahl, S. (September, 2001). How vulnerable is your company? *InformationWeek*, issue 853, pages 8 – 9.

Stanton, J. M.; Stam, K. R.; Mastrangelo, P.; and Jolton, Jefferey. (March, 2005). Analysis of end user security behaviors. *Computers & Security*, 24(2), pages 124 – 133.

Stone, E. (1978). *Research methods in organizational behavior*. Santa Monica, California: Goodyear Publishing.

Straub, D. W. (March, 1989). Validating instruments in IS research. *MIS Quarterly*, 13(1), pages 147 – 169.

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

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

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

Strous, L. (2002). The way forward. In Gertz, M.; Guldentops, E.; and Strous, L. (eds.), *Integrity, Internal Control and Security in Information Systems: Connecting governance and technology*. Norwell, Massachusetts: Kluwer Academic Publishers, pages 197 - 200.

Swanson, M. (November, 2001). Security self-assessment guide for information technology systems. *NIST Special Publication 800-26*, National Institute of Standards and Technology, U.S. Department of Commerce, Washington DC: U.S. Government Printing Office.

Templeton, G. F. (2000). *Development of the organizational learning construct and measure*. Unpublished doctoral dissertation, Auburn University, Alabama.

Templeton, G. and Snyder, C. (1997). Toward a method for providing database structures derived from an ontological specification process: The example of knowledge management. Online http://www.dfki.uni-kl.de/~aabecker/Freiburg/Final/Templeton/ontpaper.html, 12 pages, accessed 3/21/2005.

Teng, J. T. C.; Grover, V.; and Güttler, W. (February, 2002). Information technology innovations: General diffusion patterns and its relationships to innovation characteristics. *IEEE Transactions on Engineering Management*, 49(1), pages 13 – 27.

Teo, T. S. H. and King, W. R. (Summer, 1997). Integration between business planning and information systems planning: An evolutionary-contingency perspective. *Journal of Management Information Systems*, 14(1), pages 185 – 214.

Terplan, Kornel (1996). *Effective management of local area networks: Functions, instruments, and people* (Second Edition). New York: McGraw-Hill.

Thatcher, J. B. and Perrewé, P. L. (December, 2002). An empirical examination of individual traits as antecedents to computer anxiety and computer self-efficacy. *MIS Quarterly*, 26(4), pages 381 – 396.

Thomson, K. and von Solms, R. (January, 2005). Information security obedience: A definition. *Computers & Security*, 24(1), pages 69 – 75.

Thomson, M. E. and von Solms, R. (1998). Information security awareness: Educating your users effectively. *Information Management & Computer Security*, 6(4), pages 167 – 173.

Thompson, E. D. and Kaarst-Brown, M. L. (February, 2005). Sensitive information: A review and research agenda. *Journal of the American Society for Information Science and Technology*, 56(3), pages 245 – 257.

Trouble with homework. (May, 1994). The trouble with homework. *Canadian Insurance*, 99(5), pages 18 – 20.

Tunyaplin, S.; Lunce, S.; and Maniam, B. (April, 1998). The new generation office environment: The home office. *Industrial Management & Data Systems*, 98(4), pages 178 – 183.

Verton, D. (April, 2002). Disaster recovery planning still lags. *Computerworld*, 36(14), 10.

Vincent, C. and Camp, J. (September, 2004). Looking to the Internet for models of governance. *Ethics and Information Technology*, 6(3), pages 161 – 173.

Walters, G. J. (June, 2001). Privacy and security: An ethical analysis. *Computers and Society*, 31(2), pages 8 – 23.

Watson, R. T.; Kelly, G. G.; Galliers, R. D.; and Brancheau, J. C. (Spring, 1997). Key issues in information systems management: An international perspective. *Journal of Management Information Systems*, 13(4), pages 91-115.

Wattel, B. (2002). Business process security. In Gertz, M.; Guldentops, E.; and Strous, L. (eds.), *Integrity, Internal Control and Security in Information Systems: Connecting governance and technology*. Norwell, Massachusetts: Kluwer Academic Publishers, pages 176 - 186.

Weber, M. (1978). *Economy and Society*. Roth, G. and Wittich, C. (eds.). Berkeley: University of California Press.

Weber, R. (1985). *Basic Content Analysis*. London: Sage Publications.

Weber, R. (1988). *EDP auditing: Conceptual foundations and practice*. New York: McGraw-Hill Publishing, Incorporated.

Webster, J. and Compeau, D. (November, 1996). Computer-assisted versus paper-and-pencil administration of questionnaires. *Behavior Research Methods, Instruments, and Computers*, 28(4), pages 567 – 576.

White, C. E. and Christy, D. P. (December, 1987). The information center concept: A normative model and a study of six installations. *MIS Quarterly*, 11(4), pages 451 – 460.

Whitman, M. E. and Mattord, H. J. (2004). *Management of Information Security*. Boston: Thomson Course Technology.

Whitman, M. E. and Mattord, H. J. (2005). *Principles of Information Security* (Second Edition). Boston: Thomson Course Technology.

Wilson, T. (November, 2004). 3rd annual reader survey: “We’re not just geeks.” *Network Computing*, 15(22), pages 39 – 52.

Wu, L. and Rocheleau, B. (June, 2001). Formal versus informal end user training in public and private sector organizations. *Public Performance & Management Review*, 24(4), pages 312 – 321.

Zhou, X. (March, 1998). The dynamics of organizational rules. *American Journal of Sociology*, 98(5), pages 1094-1133.

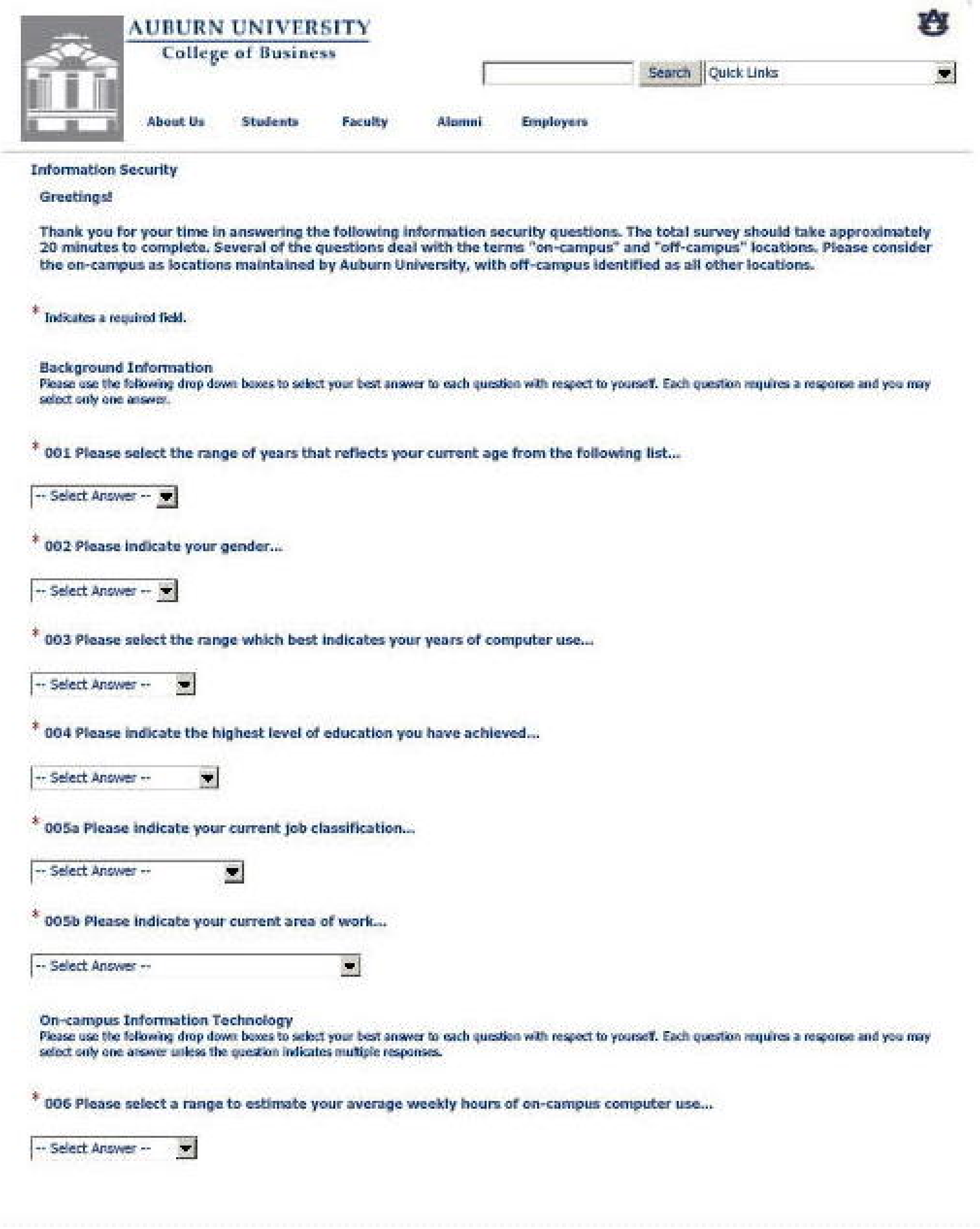
Zmud, R. W. and Boynton, A. C. (1991). Survey measures and instruments in MIS: Inventory and appraisal. In Kraemer, K. L. (ed.), *The Information systems research challenge: Survey research methods*, Volume 3. Boston, Massachusetts: Harvard Business School, pages 149 - 165.

Zviran, M. and Haga, W. J. (Spring, 1999). Password security: An empirical study. *Journal of Management Information Systems*, 15(4), pages 161 – 185.

APPENDICES

APPENDIX A

SURVEY INSTRUMENT



Information Security

Greetings!

Thank you for your time in answering the following information security questions. The total survey should take approximately 20 minutes to complete. Several of the questions deal with the terms "on-campus" and "off-campus" locations. Please consider the on-campus as locations maintained by Auburn University, with off-campus identified as all other locations.

* Indicates a required field.

Background Information
Please use the following drop down boxes to select your best answer to each question with respect to yourself. Each question requires a response and you may select only one answer.

* 001 Please select the range of years that reflects your current age from the following list...

-- Select Answer --

* 002 Please indicate your gender...

-- Select Answer --

* 003 Please select the range which best indicates your years of computer use...

-- Select Answer --

* 004 Please indicate the highest level of education you have achieved...

-- Select Answer --

* 005a Please indicate your current job classification...

-- Select Answer --

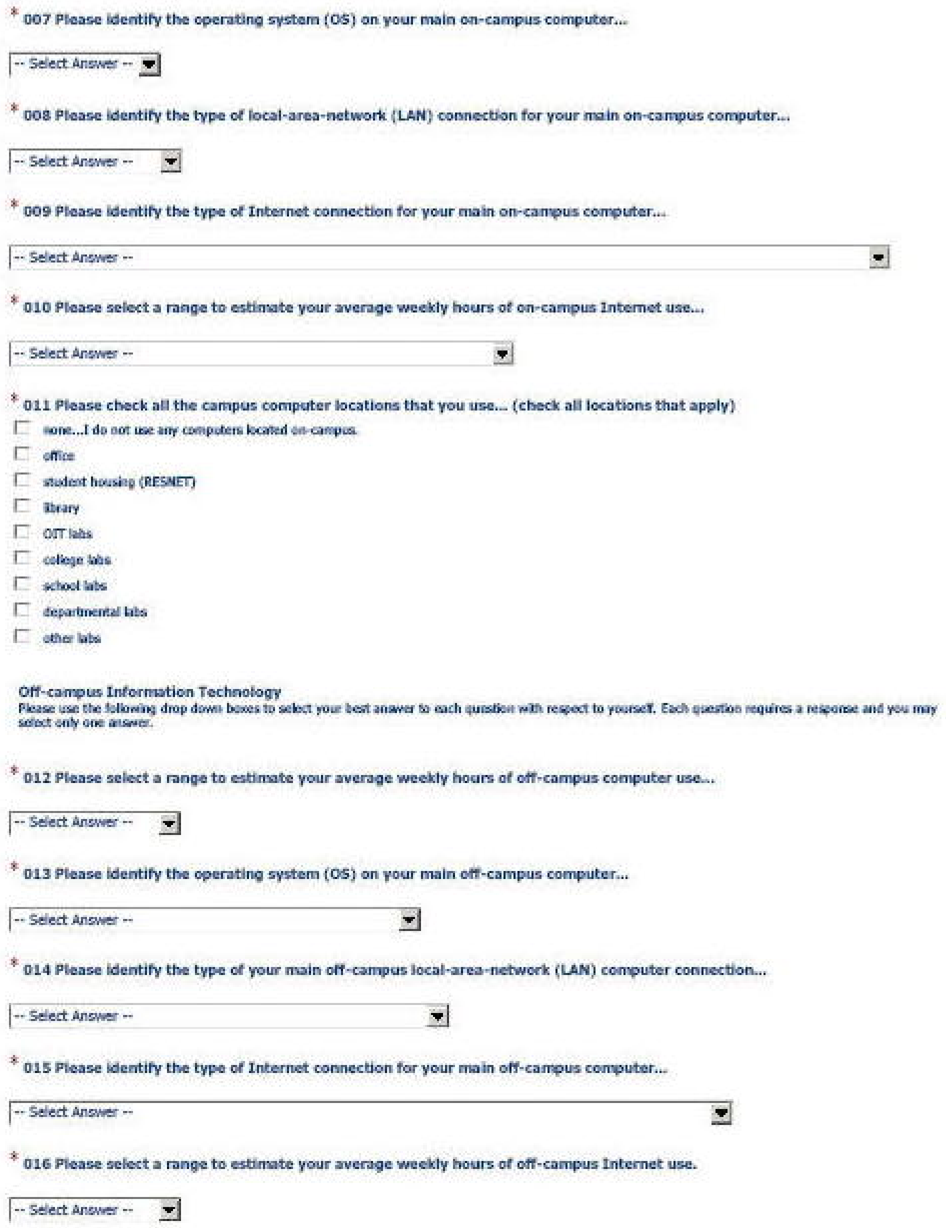
* 005b Please indicate your current area of work...

-- Select Answer --

On-campus Information Technology
Please use the following drop down boxes to select your best answer to each question with respect to yourself. Each question requires a response and you may select only one answer unless the question indicates multiple responses.

* 006 Please select a range to estimate your average weekly hours of on-campus computer use...

-- Select Answer --



* 007 Please identify the operating system (OS) on your main on-campus computer...

* 008 Please identify the type of local-area-network (LAN) connection for your main on-campus computer...

* 009 Please identify the type of Internet connection for your main on-campus computer...

* 010 Please select a range to estimate your average weekly hours of on-campus Internet use...

* 011 Please check all the campus computer locations that you use... (check all locations that apply)

- □ none...I do not use any computers located on-campus.
- □ office
- □ student housing (RESNET)
- □ library
- □ OIT labs
- □ college labs
- □ school labs
- □ departmental labs
- □ other labs

Off-campus Information Technology

Please use the following drop down boxes to select your best answer to each question with respect to yourself. Each question requires a response and you may select only one answer.

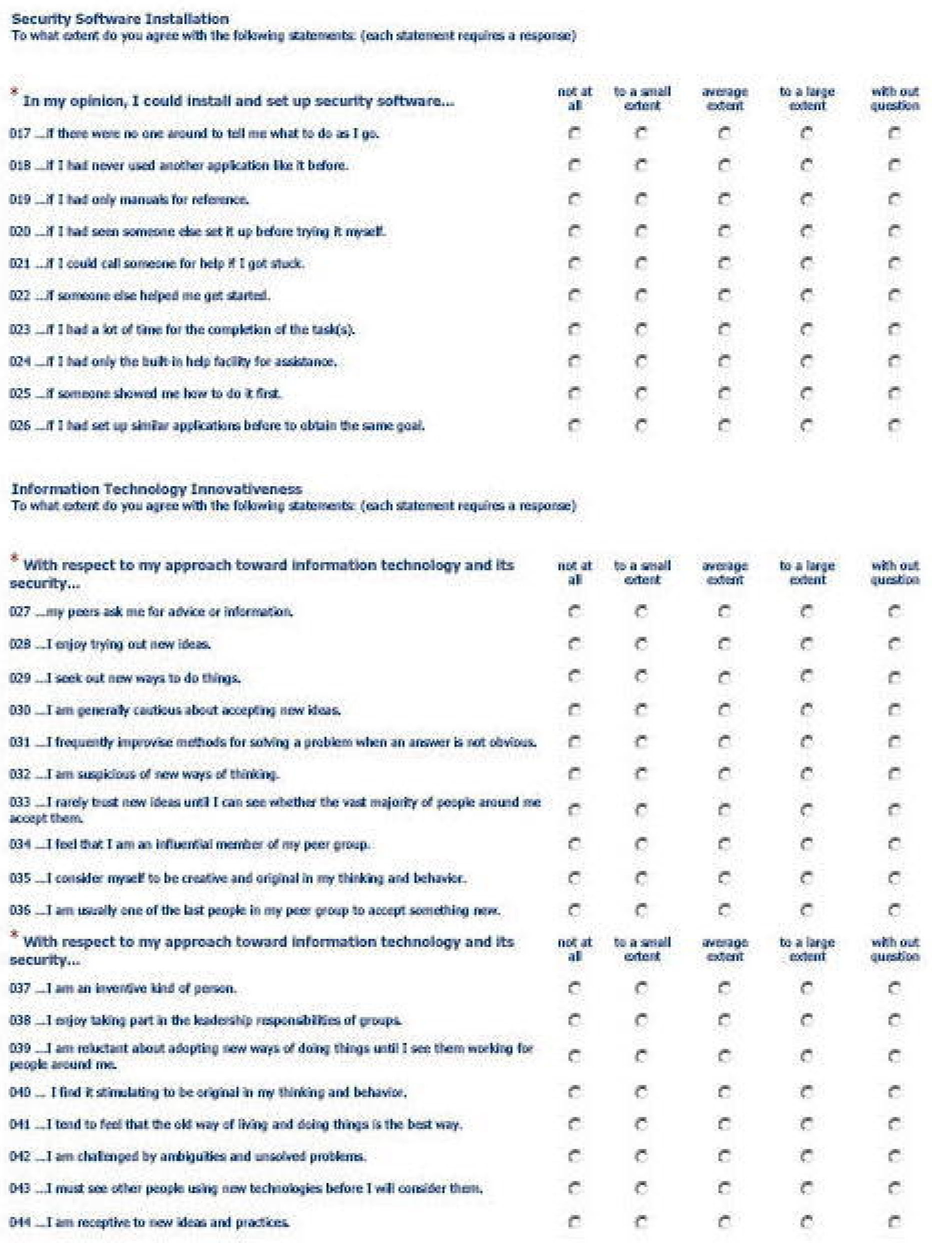
* 012 Please select a range to estimate your average weekly hours of off-campus computer use...

* 013 Please identify the operating system (OS) on your main off-campus computer...

* 014 Please identify the type of your main off-campus local-area-network (LAN) computer connection...

* 015 Please identify the type of Internet connection for your main off-campus computer...

* 016 Please select a range to estimate your average weekly hours of off-campus Internet use.

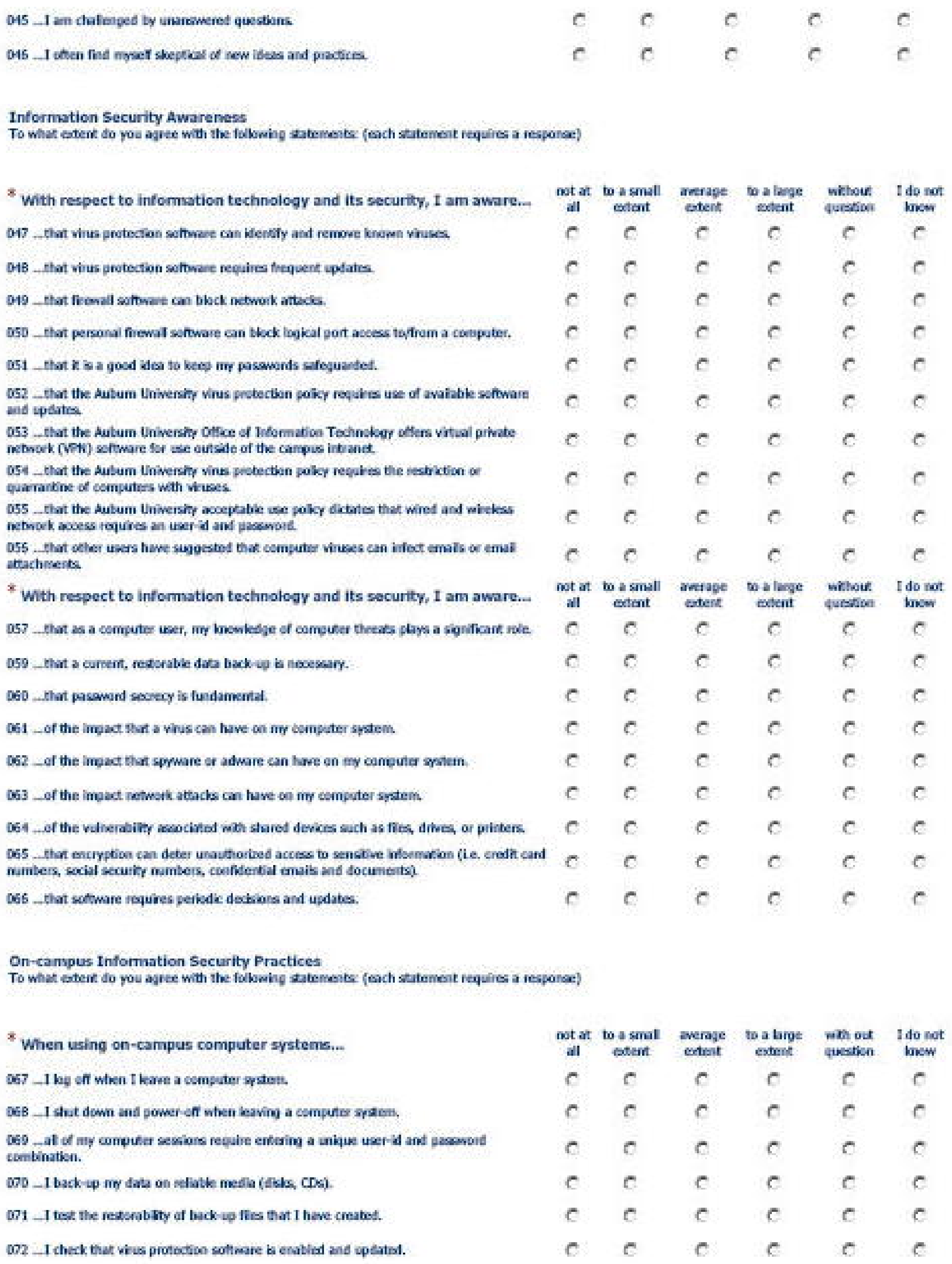


Security Software Installation
To what extent do you agree with the following statements: (each statement requires a response)

* In my opinion, I could install and set up security software...	not at all	to a small extent	average extent	to a large extent	with out question
017 ...if there were no one around to tell me what to do as I go.	○	○	○	○	○
018 ...if I had never used another application like it before.	○	○	○	○	○
019 ...if I had only manuals for reference.	○	○	○	○	○
020 ...if I had seen someone else set it up before trying it myself.	○	○	○	○	○
021 ...if I could call someone for help if I got stuck.	○	○	○	○	○
022 ...if someone else helped me get started.	○	○	○	○	○
023 ...if I had a lot of time for the completion of the task(s).	○	○	○	○	○
024 ...if I had only the built-in help facility for assistance.	○	○	○	○	○
025 ...if someone showed me how to do it first.	○	○	○	○	○
026 ...if I had set up similar applications before to obtain the same goal.	○	○	○	○	○

Information Technology Innovativeness
To what extent do you agree with the following statements: (each statement requires a response)

* With respect to my approach toward information technology and its security...	not at all	to a small extent	average extent	to a large extent	with out question
027 ...my peers ask me for advice or information.	○	○	○	○	○
028 ...I enjoy trying out new ideas.	○	○	○	○	○
029 ...I seek out new ways to do things.	○	○	○	○	○
030 ...I am generally cautious about accepting new ideas.	○	○	○	○	○
031 ...I frequently improvise methods for solving a problem when an answer is not obvious.	○	○	○	○	○
032 ...I am suspicious of new ways of thinking.	○	○	○	○	○
033 ...I rarely trust new ideas until I can see whether the vast majority of people around me accept them.	○	○	○	○	○
034 ...I feel that I am an influential member of my peer group.	○	○	○	○	○
035 ...I consider myself to be creative and original in my thinking and behavior.	○	○	○	○	○
036 ...I am usually one of the last people in my peer group to accept something new.	○	○	○	○	○
* With respect to my approach toward information technology and its security...	not at all	to a small extent	average extent	to a large extent	with out question
037 ...I am an inventive kind of person.	○	○	○	○	○
038 ...I enjoy taking part in the leadership responsibilities of groups.	○	○	○	○	○
039 ...I am reluctant about adopting new ways of doing things until I see them working for people around me.	○	○	○	○	○
040 ... I find it stimulating to be original in my thinking and behavior.	○	○	○	○	○
041 ...I tend to feel that the old way of living and doing things is the best way.	○	○	○	○	○
042 ...I am challenged by ambiguities and unsolved problems.	○	○	○	○	○
043 ...I must see other people using new technologies before I will consider them.	○	○	○	○	○
044 ...I am receptive to new ideas and practices.	○	○	○	○	○



045 ...I am challenged by unanswered questions.	○	○	○	○	○
046 ...I often find myself skeptical of new ideas and practices.	○	○	○	○	○

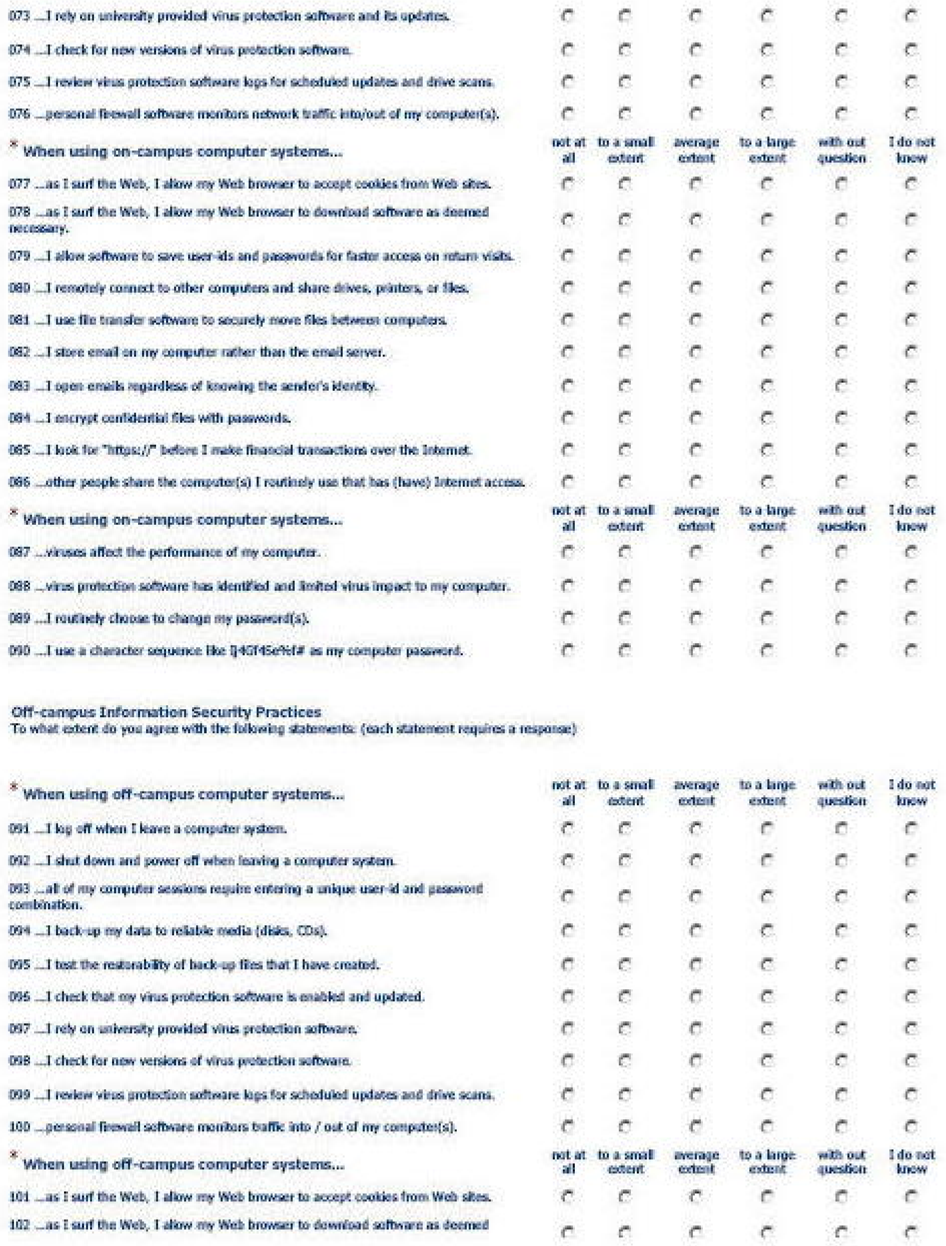
Information Security Awareness
To what extent do you agree with the following statements: (each statement requires a response)

* With respect to information technology and its security, I am aware...	not at all	to a small extent	average extent	to a large extent	without question	I do not know
047 ...that virus protection software can identify and remove known viruses.	○	○	○	○	○	○
048 ...that virus protection software requires frequent updates.	○	○	○	○	○	○
049 ...that firewall software can block network attacks.	○	○	○	○	○	○
050 ...that personal firewall software can block logical port access to/from a computer.	○	○	○	○	○	○
051 ...that it is a good idea to keep my passwords safeguarded.	○	○	○	○	○	○
052 ...that the Auburn University virus protection policy requires use of available software and updates.	○	○	○	○	○	○
053 ...that the Auburn University Office of Information Technology offers virtual private network (VPN) software for use outside of the campus intranet.	○	○	○	○	○	○
054 ...that the Auburn University virus protection policy requires the restriction or quarrantine of computers with viruses.	○	○	○	○	○	○
055 ...that the Auburn University acceptable use policy dictates that wired and wireless network access requires an user-id and password.	○	○	○	○	○	○
056 ...that other users have suggested that computer viruses can infect emails or email attachments.	○	○	○	○	○	○

* With respect to information technology and its security, I am aware...	not at all	to a small extent	average extent	to a large extent	without question	I do not know
057 ...that as a computer user, my knowledge of computer threats plays a significant role.	○	○	○	○	○	○
059 ...that a current, restorable data back-up is necessary.	○	○	○	○	○	○
060 ...that password secrecy is fundamental.	○	○	○	○	○	○
061 ...of the impact that a virus can have on my computer system.	○	○	○	○	○	○
062 ...of the impact that spyware or adware can have on my computer system.	○	○	○	○	○	○
063 ...of the impact network attacks can have on my computer system.	○	○	○	○	○	○
064 ...of the vulnerability associated with shared devices such as files, drives, or printers.	○	○	○	○	○	○
065 ...that encryption can deter unauthorized access to sensitive information (i.e. credit card numbers, social security numbers, confidential emails and documents).	○	○	○	○	○	○
066 ...that software requires periodic decisions and updates.	○	○	○	○	○	○

On-campus Information Security Practices
To what extent do you agree with the following statements: (each statement requires a response)

* When using on-campus computer systems...	not at all	to a small extent	average extent	to a large extent	with out question	I do not know
067 ...I log off when I leave a computer system.	○	○	○	○	○	○
068 ...I shut down and power-off when leaving a computer system.	○	○	○	○	○	○
069 ...all of my computer sessions require entering a unique user-id and password combination.	○	○	○	○	○	○
070 ...I back-up my data on reliable media (disks, CDs).	○	○	○	○	○	○
071 ...I test the restorability of back-up files that I have created.	○	○	○	○	○	○
072 ...I check that virus protection software is enabled and updated.	○	○	○	○	○	○



073 ...I rely on university provided virus protection software and its updates.	○	○	○	○	○	○
074 ...I check for new versions of virus protection software.	○	○	○	○	○	○
075 ...I review virus protection software logs for scheduled updates and drive scans.	○	○	○	○	○	○
076 ...personal firewall software monitors network traffic into/out of my computer(s).	○	○	○	○	○	○

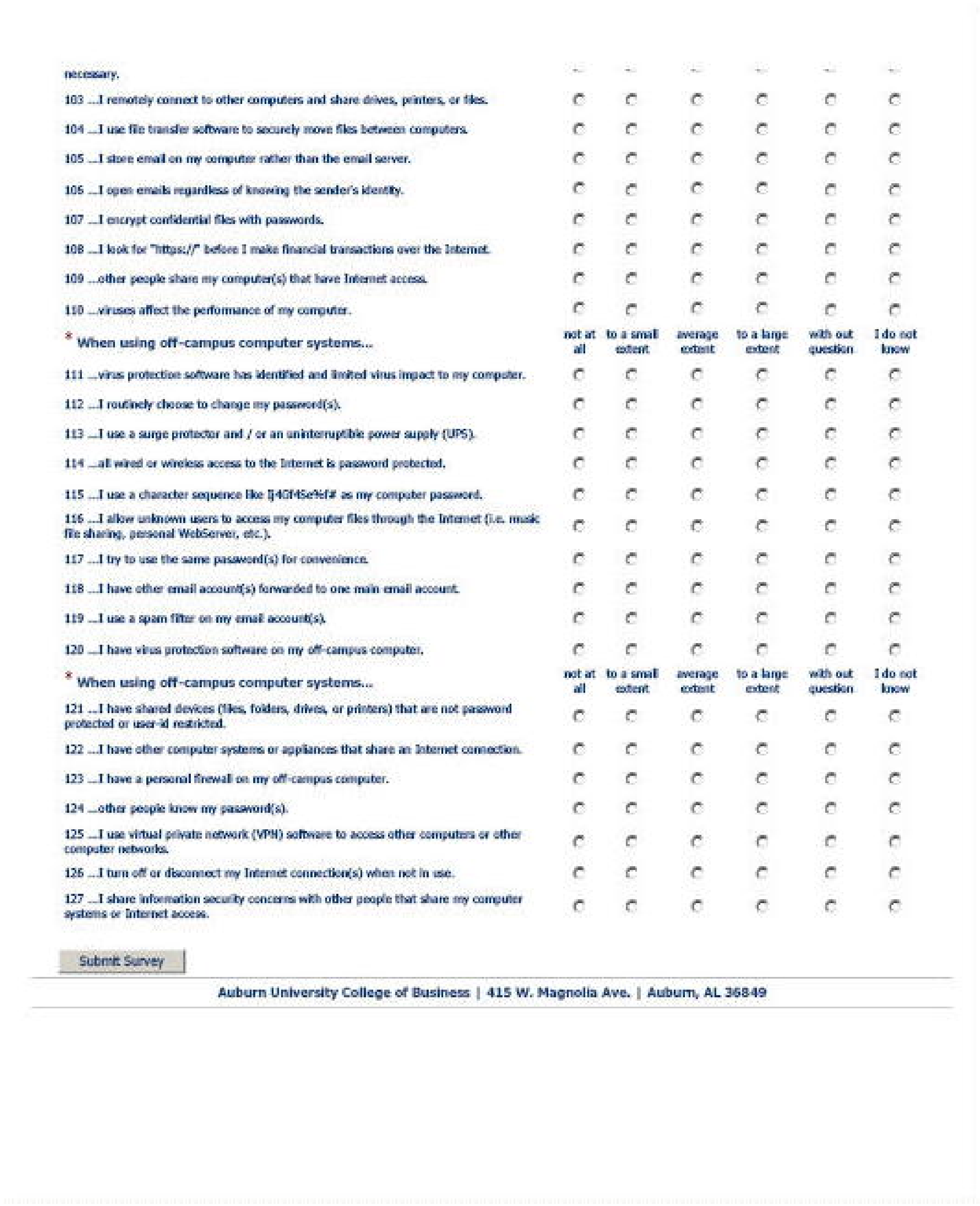
* When using on-campus computer systems...	not at all	to a small extent	average extent	to a large extent	with out question	I do not know
077 ...as I surf the Web, I allow my Web browser to accept cookies from Web sites.	○	○	○	○	○	○
078 ...as I surf the Web, I allow my Web browser to download software as deemed necessary.	○	○	○	○	○	○
079 ...I allow software to save user-ids and passwords for faster access on return visits.	○	○	○	○	○	○
080 ...I remotely connect to other computers and share drives, printers, or files.	○	○	○	○	○	○
081 ...I use file transfer software to securely move files between computers.	○	○	○	○	○	○
082 ...I store email on my computer rather than the email server.	○	○	○	○	○	○
083 ...I open emails regardless of knowing the sender's identity.	○	○	○	○	○	○
084 ...I encrypt confidential files with passwords.	○	○	○	○	○	○
085 ...I look for "https://" before I make financial transactions over the Internet.	○	○	○	○	○	○
086 ...other people share the computer(s) I routinely use that has (have) Internet access.	○	○	○	○	○	○

* When using on-campus computer systems...	not at all	to a small extent	average extent	to a large extent	with out question	I do not know
087 ...viruses affect the performance of my computer.	○	○	○	○	○	○
088 ...virus protection software has identified and limited virus impact to my computer.	○	○	○	○	○	○
089 ...I routinely choose to change my password(s).	○	○	○	○	○	○
090 ...I use a character sequence like Ij4Gf45e%f# as my computer password.	○	○	○	○	○	○

Off-campus Information Security Practices
To what extent do you agree with the following statements: (each statement requires a response)

* When using off-campus computer systems...	not at all	to a small extent	average extent	to a large extent	with out question	I do not know
091 ...I log off when I leave a computer system.	○	○	○	○	○	○
092 ...I shut down and power off when leaving a computer system.	○	○	○	○	○	○
093 ...all of my computer sessions require entering a unique user-id and password combination.	○	○	○	○	○	○
094 ...I back-up my data to reliable media (disks, CDs).	○	○	○	○	○	○
095 ...I test the restorability of back-up files that I have created.	○	○	○	○	○	○
096 ...I check that my virus protection software is enabled and updated.	○	○	○	○	○	○
097 ...I rely on university provided virus protection software.	○	○	○	○	○	○
098 ...I check for new versions of virus protection software.	○	○	○	○	○	○
099 ...I review virus protection software logs for scheduled updates and drive scans.	○	○	○	○	○	○
100 ...personal firewall software monitors traffic into / out of my computer(s).	○	○	○	○	○	○

* When using off-campus computer systems...	not at all	to a small extent	average extent	to a large extent	with out question	I do not know
101 ...as I surf the Web, I allow my Web browser to accept cookies from Web sites.	○	○	○	○	○	○
102 ...as I surf the Web, I allow my Web browser to download software as deemed	○	○	○	○	○	○



necessary.						
103 ...I remotely connect to other computers and share drives, printers, or files.	○	○	○	○	○	○
104 ...I use file transfer software to securely move files between computers.	○	○	○	○	○	○
105 ...I store email on my computer rather than the email server.	○	○	○	○	○	○
106 ...I open emails regardless of knowing the sender's identity.	○	○	○	○	○	○
107 ...I encrypt confidential files with passwords.	○	○	○	○	○	○
108 ...I look for "https://" before I make financial transactions over the Internet.	○	○	○	○	○	○
109 ...other people share my computer(s) that have Internet access.	○	○	○	○	○	○
110 ...viruses affect the performance of my computer.	○	○	○	○	○	○
* When using off-campus computer systems...	not at all	to a small extent	average extent	to a large extent	with out question	I do not know
111 ...virus protection software has identified and limited virus impact to my computer.	○	○	○	○	○	○
112 ...I routinely choose to change my password(s).	○	○	○	○	○	○
113 ...I use a surge protector and / or an uninterruptible power supply (UPS).	○	○	○	○	○	○
114 ...all wired or wireless access to the Internet is password protected.	○	○	○	○	○	○
115 ...I use a character sequence like Ij4Of4Se%f# as my computer password.	○	○	○	○	○	○
116 ...I allow unknown users to access my computer files through the Internet (i.e. music file sharing, personal WebServer, etc.).	○	○	○	○	○	○
117 ...I try to use the same password(s) for convenience.	○	○	○	○	○	○
118 ...I have other email account(s) forwarded to one main email account.	○	○	○	○	○	○
119 ...I use a spam filter on my email account(s).	○	○	○	○	○	○
120 ...I have virus protection software on my off-campus computer.	○	○	○	○	○	○
* When using off-campus computer systems...	not at all	to a small extent	average extent	to a large extent	with out question	I do not know
121 ...I have shared devices (files, folders, drives, or printers) that are not password protected or user-id restricted.	○	○	○	○	○	○
122 ...I have other computer systems or appliances that share an Internet connection.	○	○	○	○	○	○
123 ...I have a personal firewall on my off-campus computer.	○	○	○	○	○	○
124 ...other people know my password(s).	○	○	○	○	○	○
125 ...I use virtual private network (VPN) software to access other computers or other computer networks.	○	○	○	○	○	○
126 ...I turn off or disconnect my Internet connection(s) when not in use.	○	○	○	○	○	○
127 ...I share information security concerns with other people that share my computer systems or Internet access.	○	○	○	○	○	○

Auburn University College of Business | 415 W. Magnolia Ave. | Auburn, AL 36849

APPENDIX B

PILOT STUDY RESPONSES AND FREQUENCIES

Background Information

001 Please choose the interval below which includes your age...

	below 19	19 - 24	25 - 29	30 - 34	35 - 39	40 - 44	45 - 49	50 - 54	55 - 59	60 - 64	over 64
% of responses	0	97	2	1	0	0	0	0	0	0	0

002 Please indicate your gender...

	female	male
% of responses	45	55

003 Please select the range which best indicates your years of computer use...

	< 1	1 - 3	4 - 6	7 - 10	11 - 13	14 - 16	17 - 20	21 - 25	26 - 30	> 30
% of responses	0	14	47	47	22	11	2	0	0	0

004Please indicate your current college classification...

	FR	SO	JR	SR	Grad
% of responses	0	1	52	47	0

005 Please indicate your current major...

	ACCT	AVMGT	LOG	ECON	FINC	Grad	MNGT	ISM	MKTG	Other
% of responses	29	0	1	0	3	0	14	6	31	16

On-campus Information Technology

006 Please select a range to estimate your average weekly hours of on-campus computer use...

	none	< 1	1 - 5	6 - 10	11 - 15	16 - 20	21 - 25	26 - 30	31 - 35	36 - 40	> 40
% of responses	5	22	58	10	3	0	0	1	0	0	0

007 Please identify the operating system (OS) on your main on-campus computer...

	DOS	Linux	Mac	WIN 3.1	WIN 95	WIN 98	WIN NT	WIN 2000	WIN ME	WIN XP	Do not know	Not applicable
% of responses	0	0	0	0	0	2	1	3	0	71	19	4

008 Please identify the type of local-area-network (LAN) connection for your main on-campus computer...

	do not know	none	hub router	wireless router combo
% of responses	66	5	14	15

009 Please identify the type of Internet connection for your main on-campus computer...

	do not know.	not applicable	dial up	wired	wireless
% of responses	37	9	0	40	14

010 Please select a range to estimate your average weekly hours of on-campus Internet use...

	not applicable	none	< 1	1 - 5	6 - 10	11 - 15	16 - 20	21 - 25	26 - 30	31 - 35	36 - 40	> 40
% of responses	5	2	25	57	9	1	0	0	0	0	0	0

011 Please check all the on-campus computer locations that you use...

	none	office	RESNET	library	OIT labs	college labs	school labs	Dept. labs	other labs
% of responses	5	8	3	60	60	60	42	24	6

Off-campus Information Technology

012 Please select a range to estimate your average weekly hours of off-campus computer use...

	none	< 1	1 - 5	6 - 10	11 - 15	16 - 20	21 - 25	26 - 30	31 - 35	36 - 40	> 40
% of responses	1	4	24	27	17	10	6	5	1	2	2

013 Please identify the operating system (OS) on your main off-campus computer...

	Do not know	NA	DOS	Linux	Mac	WIN 3.1	WIN 95	WIN 98	WIN NT	WIN 2000	WIN ME	WIN XP
% of responses	3	2	0	0	1	0	0	3	0	5	3	82

014 Please identify the type of local-area-network (LAN) connection for your main off-campus computer...

	do not know	none	hub router	wireless router combo
% of responses	21	8	21	49

015 Please identify the type of Internet connection for your main off-campus computer...

	not applicable	do not know.	none	dial up	DSL	Cable	Satellite
% of responses	2.4	3.5	1.0	3.1	18.5	69.9	1.4

016 Please select a range to estimate your average weekly hours of off-campus Internet use...

	none	< 1	1 - 5	6 - 10	11 - 15	16 - 20	21 - 25	26 - 30	31 - 35	36 - 40	> 40
% of responses	3	5	24	30	15	9	7	3	2	2	2

Security Software Installation (alpha = 0.95)

To what extent do you agree with the following statements: (each statement requires a response)

		Percent of Responses				
* In my opinion, I could install and set up security software...	Average	not at all	to a small extent	average extent	to a large extent	with out question
017 ...if there were no one around to tell me what to do as I go.	2.89	18	24	24	19	15
018 ...if I had never used another application like it before.	2.78	19	28	22	19	13
019 ...if I had only manuals for reference.	3.43	5	18	28	26	23
020 ...if I had seen someone else set it up before trying it myself.	3.53	5	15	27	31	23
021 ...if I could call someone for help if I got stuck.	3.80	3	10	25	30	33
022 ...if someone else helped me get started.	3.78	3	7	25	37	27
023 ...if I had a lot of time for the completion of the task(s).	3.69	3	11	27	30	29
024 ...if I had only the built-in help facility for assistance.	3.37	6	19	28	27	20
025 ...if someone showed me how to do it first.	4.02	2	6	20	31	41
026 ...if I had set up similar applications before to obtain the same goal.	3.90	2	9	21	34	34

Information Technology Innovativeness (alpha = .84) (original eight alpha =.77) (added twelve alpha = .88)

To what extent do you agree with the following statements: (each statement requires a response)

		Percent of Responses				
* With respect to my approach toward information technology and its security…	Average	not at all	to a small extent	average extent	to a large extent	with out question
027 ...my peers ask me for advice or information.	2.48	24	29	29	11	7
028 ...I enjoy trying out new ideas.	2.99	9	24	36	22	10
029 ...I seek out new ways to do things.	2.87	10	28	33	23	6
030 ...I am generally cautious about accepting new ideas.	2.73	7	35	39	15	4
031 ...I frequently improvise methods for solving a problem when an answer is not obvious.	2.89	9	25	40	20	6
032 ...I am suspicious of new ways of thinking.	2.46	14	41	33	9	3
033 ...I rarely trust new ideas until I can see whether the vast majority of people around me accept them.	2.45	16	39	31	13	1
034 ...I feel that I am an influential member of my peer group.	3.10	6	17	44	25	7
035 ...I consider myself to be creative and original in my thinking and behavior.	3.30	5	13	41	30	11
036 ...I am usually one of the last people in my peer group to accept something new.	2.13	29	39	25	5	2
037 ...I am an inventive kind of person.	2.71	11	30	40	15	5
038 ...I enjoy taking part in the leadership responsibilities of groups.	3.11	8	19	36	27	10
039 ...I am reluctant about adopting new ways of doing things until I see them working for people around me.	2.54	9	41	38	10	2
040 ... I find it stimulating to be original in my thinking and behavior.	3.26	3	17	38	32	9
041 ...I tend to feel that the old way of living and doing things is the best way.	2.27	17	47	28	6	2
042 ...I am challenged by ambiguities and unsolved problems.	2.93	7	25	41	21	6
043 ...I must see other people using new technologies before I will consider them.	2.42	16	42	28	12	2
044 ...I am receptive to new ideas and practices.	3.36	3	10	44	32	10
045 ...I am challenged by unanswered questions.	3.12	5	18	45	25	7
046 ...I often find myself skeptical of new ideas and practices.	2.49	11	42	36	8	3

Response percentage of 20% or higher

Information Security Awareness (alpha = .92)

To what extent do you agree with the following statements: (each statement requires a response)

		Percent of Responses					
* With respect to information technology and its security, I am aware...	Average	not at all	to a small extent	average extent	to a large extent	with out question	I do not know
047 ...that virus protection software can identify and remove known viruses.	4.07	2	3	17	31	45	2
048 ...that virus protection software requires frequent updates.	4.16	2	4	13	29	50	2
049 ...that firewall software can block network attacks.	3.47	3	8	20	27	32	10
050 ...that personal firewall software can block logical port access to/from a computer.	3.02	5	10	18	24	25	17
051 ...that it is a good idea to keep my passwords safeguarded.	4.18	1	6	13	20	57	3
052 ...that the Auburn University virus protection policy requires use of available software and updates	3.09	7	10	20	22	27	14
053 ...that the Auburn University Office of Information Technology offers virtual private network (VPN) software for use outside of the campus intranet.	2.27	15	14	18	14	15	24
054 ...that the Auburn University virus protection policy requires the restriction or quarrantine of computes with viruses.	2.66	10	13	18	18	20	20
055 ...that the Auburn University acceptable use policy dictates that wired and wireless network access requires an user-id and password.	3.30	5	8	16	24	33	14
056 ...that other users have suggested that computer viruses can infect emails or email attachments.	3.84	2	6	16	29	41	6
057 ...that as a computer user, my knowledge of computer threats plays a significant role.	3.66	2	8	24	31	30	5
058 ...that a current, restorable data back-up is necessary.	3.41	2	11	28	27	25	7
059 ...that password secrecy is fundamental.	4.06	1	4	15	29	47	4
060 ...of the impact that a virus can have on my computer system.	4.04	1	3	16	30	46	4
061 ...of the impact that spyware or adware can have on my computer system.	3.91	2	5	21	27	42	3
062 ...of the impact network attacks can have on my computer system.	3.48	2	11	26	24	30	7
063 ...of the vulnerability associated with shared devices such as files, drives, or printers.	3.41	3	11	26	24	28	7
064 ...that encryption can deter unauthorized access to sensitive information (i.e. credit card numbers, social security numbers, confidential emails and documents).	3.29	4	10	21	24	29	12
065 ...that software requires periodic decisions and updates.	3.80	1	7	20	33	35	5

"I do not know" percentage of 10% or higher

On-campus Information Security Practices (alpha = .83)

To what extent do you agree with the following statements: (each statement requires a response)

		Percent of Responses					
* When using on-campus computer systems...	Average	not at all	to a small extent	average extent	to a large extent	with out question	I do not know
066 ...I log off when I leave a computer system.	4.52	2	1	5	7	80	4
067 ...I shut down and power-off when leaving a computer system.	1.64	67	11	7	7	5	3
068 ...all of my computer sessions require entering a unique user-id and password combination.	4.31	3	2	7	14	70	4
069 ...I back-up my data on reliable media (disks, CDs).	2.72	23	20	21	18	15	4
070 ...I test the restorability of back-up files that I have created.	2.36	34	20	15	11	14	5
071 ...I check that virus protection software is enabled and updated.	2.19	44	14	15	11	11	4
072 ...I rely on university provided virus protection software and its updates.	3.57	12	7	14	22	40	5
073 ...I check for new versions of virus protection software.	1.97	50	17	14	9	7	3
074 ...I review virus protection software logs for scheduled updates and drive scans.	1.89	55	13	11	9	7	3
075 ...personal firewall software monitors network traffic into/out of my computer(s).	2.06	34	11	14	13	11	17
076 ...as I surf the Web, I allow my Web browser to accept cookies from Web sites.	2.16	7	20	20	14	15	24
077 ...as I surf the Web, I allow my Web browser to download software as deemed necessary.	2.37	6	19	22	22	23	9
078 ...I allow software to save user-ids and passwords for faster access on return visits.	1.66	3	10	10	11	60	6
079 ...I remotely connect to other computers and share drives, printers, or files.	1.79	4	8	17	17	44	11
080 ...I use file transfer software to securely move files between computers.	1.72	43	14	19	8	3	14
081 ...I store email on my computer rather than the email server.	1.50	3	7	9	13	52	15
082 ...I open emails regardless of knowing the sender's identity.	1.72	51	23	11	7	3	5
083 ...I encrypt confidential files with passwords.	1.71	45	12	15	5	7	15
084 ...I look for "https://" before I make financial transactions over the Internet.	2.10	31	10	17	9	15	18
085 ...other people share the computer(s) I routinely use that has (have) Internet access.	2.79	24	16	17	11	20	11
086 ...viruses affect the performance of my computer.	2.15	16	9	14	14	28	19
087 ...virus protection software has identified and limited virus impact to my computer.	2.44	13	11	18	13	21	24
088 ...I routinely choose to change my password(s).	1.84	45	25	17	3	5	5
089 ...I use a character sequence like Ij4Gf4Se%f# as my computer password.	1.72	61	14	10	5	7	4

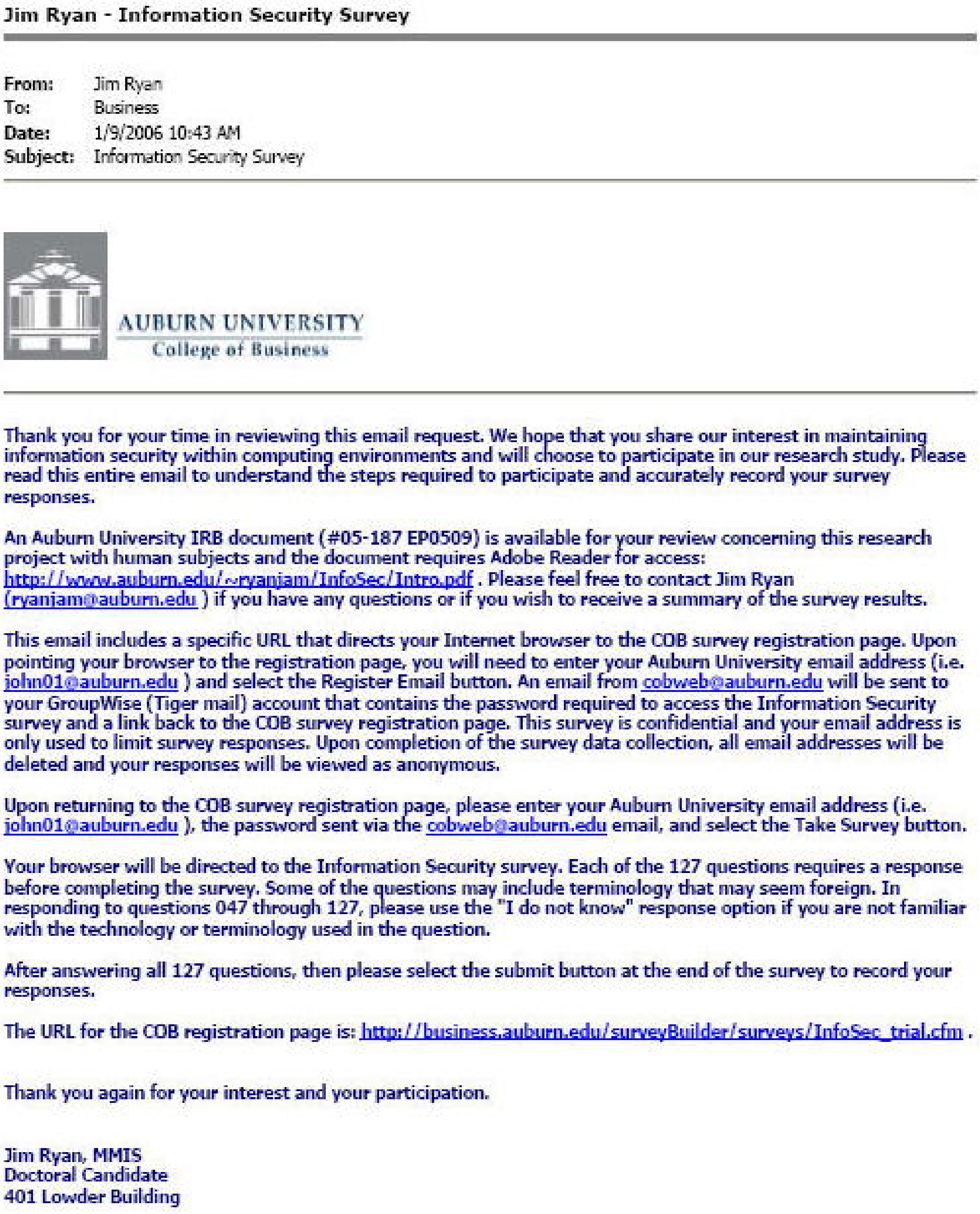
Off-campus Information Security Practices (alpha = .88)

To what extent do you agree with the following statements: (each statement requires a response)

		Percent of Responses					
* When using off-campus computer systems...	Average	not at all	to a small extent	average extent	to a large extent	with out question	I do not know
090 ...I log off when I leave a computer system.	2.47	36	18	15	12	16	2
091 ...I shut down and power off when leaving a computer system.	2.37	36	21	16	12	13	2
092 ...all of my computer sessions require entering a unique user-id and password combination.	2.68	32	15	16	16	18	2
093 ...I back-up my data to reliable media (disks, CDs).	2.69	22	24	22	16	14	2
094 ...I test the restorability of back-up files that I have created.	2.51	27	23	17	13	15	5
095 ...I check that my virus protection software is enabled and updated.	3.31	11	13	25	20	28	3
096 ...I rely on university provided virus protection software.	2.11	44	12	20	8	10	6
097 ...I check for new versions of virus protection software.	3.03	17	15	24	15	25	4
098 ...I review virus protection software logs for scheduled updates and drive scans.	2.84	21	17	24	14	20	4
099 ...personal firewall software monitors traffic into / out of my computer(s).	2.66	14	11	17	14	24	19
100 ...as I surf the Web, I allow my Web browser to accept cookies from Web sites.	2.23	5	16	26	22	11	20
101 ...as I surf the Web, I allow my Web browser to download software as deemed necessary.	2.48	6	16	29	29	13	8
102 ...I remotely connect to other computers and share drives, printers, or files.	1.93	5	7	20	23	37	9
103 ...I use file transfer software to securely move files between computers.	1.95	32	21	18	8	7	14
104 ...I store email on my computer rather than the email server.	1.85	7	9	13	16	44	11
105 ...I open emails regardless of knowing the sender's identity.	1.68	2	4	12	27	49	5
106 ...I encrypt confidential files with passwords.	1.93	40	20	15	7	8	10
107 ...I look for "https://" before I make financial transactions over the Internet.	2.36	26	14	20	9	17	14
108 ...other people share my computer(s) that have Internet access.	2.40	12	13	20	21	25	8
109 ...viruses affect the performance of my computer.	2.74	20	18	20	10	23	8
110 ...virus protection software has identified and limited virus impact to my computer.	3.20	4	12	22	25	25	12
111 ...I routinely choose to change my password(s).	2.06	38	26	18	9	5	3
112 ...I use a surge protector and / or an uninterruptible power supply (UPS).	3.55	8	5	16	13	48	10
113 ...all wired or wireless access to the Internet is password protected.	2.62	20	12	20	9	25	15
114 ...I use a character sequence like Ij4Gf4Se%f# as my computer password.	1.99	52	14	15	6	10	3
115 ...I allow unknown users to access my computer files through the Internet (i.e. music, file sharing, personal Web Server, etc.).	1.93	6	8	16	19	45	6
116 ...I try to use the same password(s) for convenience.	3.15	20	25	21	23	9	3
117 ...I have other email account(s) forwarded to one main email account.	1.63	3	6	11	13	63	3
118 ...I use a spam filter on my email account(s).	2.81	17	13	21	17	22	11
119 ...I have virus protection software on my off-campus computer.	3.94	3	4	18	15	54	6
120 ...I have shared devices (files, folders, drives, or printers) that are not password protected or user restricted.	2.33	7	16	24	18	24	10
121 ...I have other computer systems or appliances that share an Internet connection.	2.12	8	11	23	12	32	13
122 ...I have a personal firewall on my off-campus computer.	2.81	11	9	15	13	31	21
123 ...other people know my password(s).	1.64	2	3	12	24	53	5
124 ...I use virtual private network (VPN) software to access other computers or other computer networks.	1.22	37	7	11	5	3	36
125 ...I turn off or disconnect my Internet connection(s) when not in use.	2.03	46	17	14	8	10	5
126 ...I share information security concerns with other people that share my computer systems or Internet access.	2.02	32	24	20	9	6	10

APPENDIX C

INTRODUCTION EMAIL



Jim Ryan - Information Security Survey

From: Jim Ryan
To: Business
Date: 1/9/2006 10:43 AM
Subject: Information Security Survey

AUBURN UNIVERSITY
College of Business

Thank you for your time in reviewing this email request. We hope that you share our interest in maintaining information security within computing environments and will choose to participate in our research study. Please read this entire email to understand the steps required to participate and accurately record your survey responses.

An Auburn University IRB document (#05-187 EP0509) is available for your review concerning this research project with human subjects and the document requires Adobe Reader for access: http://www.auburn.edu/~ryanjam/InfoSec/Intro.pdf . Please feel free to contact Jim Ryan (ryanjam@auburn.edu) if you have any questions or if you wish to receive a summary of the survey results.

This email includes a specific URL that directs your Internet browser to the COB survey registration page. Upon pointing your browser to the registration page, you will need to enter your Auburn University email address (i.e. john01@auburn.edu) and select the Register Email button. An email from cobweb@auburn.edu will be sent to your GroupWise (Tiger mail) account that contains the password required to access the Information Security survey and a link back to the COB survey registration page. This survey is confidential and your email address is only used to limit survey responses. Upon completion of the survey data collection, all email addresses will be deleted and your responses will be viewed as anonymous.

Upon returning to the COB survey registration page, please enter your Auburn University email address (i.e. john01@auburn.edu), the password sent via the cobweb@auburn.edu email, and select the Take Survey button.

Your browser will be directed to the Information Security survey. Each of the 127 questions requires a response before completing the survey. Some of the questions may include terminology that may seem foreign. In responding to questions 047 through 127, please use the "I do not know" response option if you are not familiar with the technology or terminology used in the question.

After answering all 127 questions, then please select the submit button at the end of the survey to record your responses.

The URL for the COB registration page is: http://business.auburn.edu/surveyBuilder/surveys/InfoSec_trial.cfm .

Thank you again for your interest and your participation.

Jim Ryan, MMIS
Doctoral Candidate
401 Lowder Building

APPENDIX D

INTERNAL REVIEW BOARD (IRB) INFORMATION SHEET

Department of Management
Suite 401, Lowder Building
Auburn University, Alabama 36849

Information Sheet for Research Study Entitled
"A comparison of information security trends between formal and informal environments."

You are invited to participate in a research study to investigate information security practices between business and home computing environments. This study is being conducted by Mr. James E. Ryan under the supervision of Dr. R. Kelly Rainer, Jr. We hope to learn how information security awareness affects computer practices at work and at home. You were selected as a possible participant because of your use of information technology within business and home computing environments.

If you decide to participate, we request that you respond to the email that accompanied this attachment and register your Auburn University email address. A follow-up email will be sent to your mailbox with a unique user-id key and a Web-based survey uniform resource locator (URL). By hyper-linking to the survey URL and entering the unique user-id key, you will gain access to complete our information security awareness survey. The survey should take approximately 20 minutes to complete and all questions require a response. All survey responses are confidential, all data analysis is anonymous, and no risk is associated with completing our survey. In participating in the survey, respondents may broaden their awareness of information security practices. We cannot promise you that you will receive any or all of the benefits described.

Any information obtained in connection with this study will remain confidential and the data analysis will be anonymous. Information collected through your participation may be used to fulfill an educational requirement for a doctoral dissertation, published in a professional journal, and/or presented at a professional meeting. Participants may withdraw from participation at any time prior to submitting their survey responses. After participants have submitted their confidential survey responses, the key identifiers will be destroyed and the confidential information cannot be withdrawn because there will be no way to identify individual information. Your decision whether or not to participate will not jeopardize your future relations with Auburn University or the Management Department..

If you have any questions I invite you to send them to ryanjam@auburn.edu . If you have questions later, please contact me via the same email address. I will be happy to answer them.

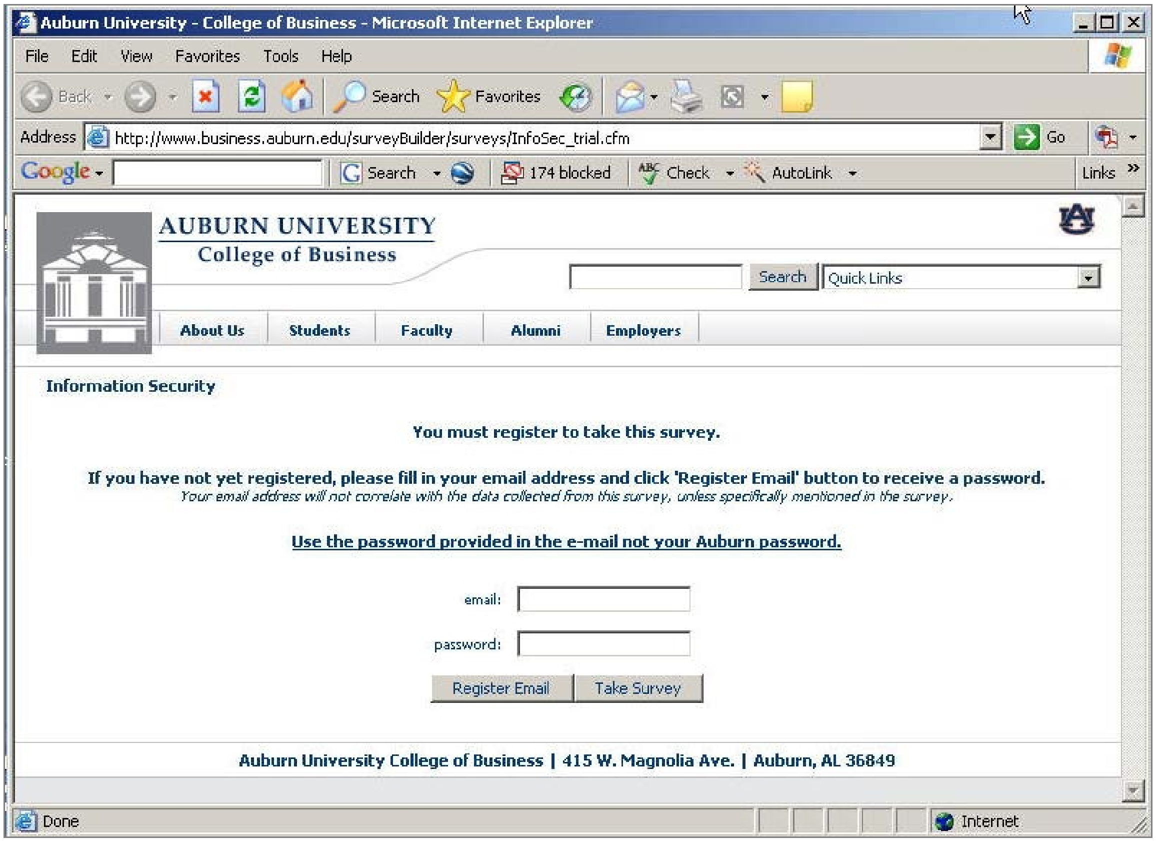
For more information regarding your rights as a research participant you may contact the Auburn University Office of Human Subjects Research or the Institutional Review Board by phone (334)-844-5966 or email at hsubjec@auburn.edu or IRBChair@auburn.edu .

HAVING READ THE INFORMATION PROVIDED, YOU MUST DECIDE WHETHER TO PARTICIPATE IN THIS RESEARCH PROJECT. IF YOU DECIDE TO PARTICIPATE, THE DATA YOU PROVIDE WILL SERVE AS YOUR AGREEMENT TO DO SO. THIS LETTER IS YOURS TO KEEP.

J. E. Ryan August 22, 2005
James E. Ryan Date
Ph.D. Candidate, Auburn University
Principal Investigator

APPENDIX E

WEB SURVEY REGISTRATION PAGE


Auburn University - College of Business - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Address
http://www.business.auburn.edu/surveyBuilder/surveys/InfoSec_trial.cfm
Go
Google
Search
174 blocked
Check
AutoLink
Links
AUBURN UNIVERSITY
College of Business
Search
Quick Links
About Us
Students
Faculty
Alumni
Employers
Done
Internet

Information Security

You must register to take this survey.

If you have not yet registered, please fill in your email address and click 'Register Email' button to receive a password.
Your email address will not correlate with the data collected from this survey, unless specifically mentioned in the survey.

Use the password provided in the e-mail not your Auburn password.

email:

password:

Register Email | Take Survey

Auburn University College of Business | 415 W. Magnolia Ave. | Auburn, AL 36849

APPENDIX F

SCALE MEASURES DESCRIPTIVE STATISTICS

Computer Self-efficacy (CSE) Scale Item-responses

Item	N	Minimum	Maximum	Mean	Standard Deviation	Skewness	Kurtosis
CSE01	531	1	5	3.12	1.28	-0.10	-1.06
CSE02	531	1	5	2.95	1.26	+0.04	-1.02
CSE03	531	1	5	3.48	1.13	-0.24	-0.85
CSE04	531	1	5	3.68	1.10	-0.54	-0.45
CSE05	531	1	5	3.97	1.03	-0.77	-0.16
CSE06	531	1	5	3.94	1.03	-0.86	+0.20
CSE07	531	1	5	3.79	1.07	-0.60	-0.36
CSE08	531	1	5	3.45	1.16	-0.31	-0.76
CSE09	531	1	5	4.13	1.01	-1.06	+0.50
CSE10	531	1	5	4.08	0.99	-0.88	+0.02

Personal Innovativeness (PI) Scale Item-responses

Item	N	Minimum	Maximum	Mean	Standard Deviation	Skewness	Kurtosis
PI01	531	1	5	2.68	1.19	+0.23	-0.76
PI02	531	1	5	3.21	1.10	-0.08	-0.71
PI03	531	1	5	3.12	1.09	-0.04	-0.70
PI04	531	1	5	2.65	0.97	+0.35	-0.25
PI05	531	1	5	3.11	1.01	-0.10	-0.51
PI06	531	1	5	2.20	0.95	+0.66	+0.29
PI07	531	1	5	2.20	0.92	+0.43	-0.41
PI08	531	1	5	3.11	0.97	-0.15	-0.04
PI09	531	1	5	3.40	0.93	-0.33	-0.01
PI10	531	1	5	1.93	0.91	+0.83	+0.45
PI11	531	1	5	2.80	1.04	+0.16	-0.40
PI12	531	1	5	3.14	1.05	-0.17	-0.54
PI13	531	1	5	2.31	0.91	+0.36	-0.24
PI14	531	1	5	3.35	0.97	-0.23	-0.35
PI15	531	1	5	2.11	0.88	+0.59	+0.26
PI16	531	1	5	3.11	1.01	-0.05	-0.46
PI17	531	1	5	2.21	0.94	+0.51	-0.17
PI18	531	1	5	3.57	0.88	-0.29	+0.04
PI19	531	1	5	3.29	0.94	-0.23	-0.15
PI20	531	1	5	2.28	0.92	+0.76	+0.70

Individual Information Security Awareness (ISA) Scale Item-responses

Item	N	Minimum	Maximum	Mean	Standard Deviation	Skewness	Kurtosis
A01	531	0	5	4.24	1.01	-1.83	+4.18
A02	531	0	5	4.40	0.98	-2.20	+5.70
A03	531	0	5	3.72	1.44	-1.34	+1.11
A04	531	0	5	3.03	1.81	-0.60	-1.03
A05	531	0	5	4.44	1.07	-2.36	+5.74
A06	531	0	5	3.60	1.64	-1.06	-0.06
A07	531	0	5	2.40	1.89	+0.09	-1.46
A08	531	0	5	2.79	1.85	-0.26	-1.37
A09	531	0	5	3.55	1.73	-1.02	-0.29
A10	531	0	5	4.14	1.27	-1.82	+3.01
A11	531	0	5	3.86	1.19	-1.28	+1.73
A12	531	0	5	3.80	1.36	-1.23	+1.06
A13	531	0	5	4.34	1.06	-2.19	+5.41
A14	531	0	5	4.28	1.07	-2.08	+5.08
A15	531	0	5	3.99	1.31	-1.62	+2.31
A16	531	0	5	3.79	1.40	-1.23	+0.92
A17	531	0	5	3.69	1.41	-1.03	+0.35
A18	531	0	5	3.66	1.55	-1.16	+0.39
A19	531	0	5	4.14	1.16	-1.74	+3.22

Information Security Practice at Work (ISP@W) Scale Item-responses

Item	N	Minimum	Maximum	Mean	Standard Deviation	Skewness	Kurtosis
W01	531	0	5	4.18	1.37	-1.67	+1.80
W02	531	0	5	2.08	1.44	+0.90	-0.42
W03	531	0	5	4.14	1.40	-1.65	+1.69
W04	531	0	5	2.84	1.49	-0.08	-1.11
W05	531	0	5	2.42	1.52	+0.41	-1.07
W06	531	0	5	2.75	1.64	+0.10	-1.40
W07	531	0	5	3.94	1.49	-1.36	+0.71
W08	531	0	5	2.42	1.52	+0.45	-1.08
W09	531	0	5	2.05	1.39	+0.85	-0.36
W10	531	0	5	2.11	1.74	+0.42	-1.18
W11	531	0	5	2.28	1.55	-0.13	-1.17
W12	531	0	5	2.36	1.31	+0.02	-0.82
W13	531	0	5	1.64	1.12	+1.19	+0.64
W14	531	0	5	1.90	1.33	+0.83	-0.14
W15	531	0	5	1.81	1.36	+0.78	-0.26
W16	531	0	5	1.77	1.41	+0.89	-0.25
W17	531	0	5	1.62	0.98	+1.27	+1.83
W18	531	0	5	1.67	1.32	+1.01	+0.41
W19	531	0	5	2.24	1.77	+0.40	-1.28
W20	531	0	5	2.26	1.59	+0.49	-1.03
W21	531	0	5	2.20	1.73	+0.48	-1.15
W22	531	0	5	2.78	1.87	-0.27	-1.38
W23	531	0	5	2.05	1.22	+0.73	+0.06
W24	531	0	5	2.05	1.48	+0.91	-0.50

Information Security Practice at Home (ISP@H) Scale Item-responses

Item	N	Minimum	Maximum	Mean	Standard Deviation	Skewness	Kurtosis
H01	531	0	5	2.85	1.61	+0.08	-1.43
H02	531	0	5	2.68	1.55	+0.28	-1.28
H02	531	0	5	2.89	1.63	+0.07	-1.50
H04	531	0	5	2.69	1.42	+0.22	-1.05
H05	531	0	5	2.44	1.51	+0.43	-1.06
H06	531	0	5	3.44	1.47	-0.59	-0.76
H07	531	0	5	2.33	1.66	+0.55	-1.20
H08	531	0	5	3.10	1.57	-0.22	-1.21
H09	531	0	5	2.65	1.53	+0.18	-1.19
H10	531	0	5	2.60	1.88	-0.04	-1.50
H11	531	0	5	2.29	1.42	-0.11	-0.82
H12	531	0	5	2.43	1.23	+0.02	-0.52
H13	531	0	5	1.80	1.21	+0.97	+0.36
H14	531	0	5	1.87	1.39	+0.83	-0.18
H15	531	0	5	1.97	1.47	+0.80	-0.54
H16	531	0	5	1.54	0.93	+1.45	+2.55
H17	531	0	5	1.82	1.37	+0.92	+0.03
H18	531	0	5	2.51	1.73	+0.21	-1.36
H19	531	0	5	2.40	1.49	+0.38	-1.01
H20	531	0	5	2.43	1.67	+0.35	-1.21
H21	531	0	5	3.23	1.67	-0.64	-0.75
H22	531	0	5	2.08	1.21	+0.77	+0.00
H23	531	0	5	3.79	1.64	-1.13	-0.08
H24	531	0	5	3.04	1.83	-0.33	-1.37
H25	531	0	5	2.23	1.56	+0.74	-0.90
H26	531	0	5	1.57	1.11	+1.56	+1.87
H27	531	0	5	3.10	1.34	-0.30	-0.76
H28	531	0	5	1.67	1.23	+1.51	+1.27
H29	531	0	5	3.13	1.72	-0.42	-1.21
H30	531	0	5	4.15	1.39	-1.72	+2.06
H31	531	0	5	2.04	1.42	+0.54	-0.84
H32	531	0	5	2.07	1.51	+0.65	-0.78
H33	531	0	5	2.83	1.99	-0.21	-1.58
H34	531	0	5	1.62	0.99	+1.41	+2.39
H35	531	0	5	1.35	1.39	+1.24	+0.78
H36	531	0	5	2.55	1.67	+0.34	-1.40
H37	531	0	5	2.40	1.55	+0.34	-1.06

Human Traits:

Descriptive Statistics

	N	Minimum	Maximum	Mean	Std. Deviation
CSE	531	1.00	5.00	3.66	0.93
PI	531	1.00	5.00	3.16	0.76
Valid N (listwise)	531				

Individual ISA Item Subscales:

Descriptive Statistics

	N	Minimum	Maximum	Mean	Std. Deviation
Technology	531	0.00	5.00	3.85	1.04
Policy	531	0.00	5.00	3.76	1.24
Threat-context	531	0.00	5.00	3.95	0.95
Valid N (listwise)	531				

ISP@W Item Subscales:

Descriptive Statistics

	N	Minimum	Maximum	Mean	Std. Deviation
Det	531	0.00	5.00	2.05	1.22
Prev	531	0.00	5.00	2.09	1.01
D-P	531	0.00	5.00	2.25	1.22
Valid N (listwise)	531				

ISP@H Item Subscales:

Descriptive Statistics

	N	Minimum	Maximum	Mean	Std. Deviation
TA	531	0.00	5.00	2.29	0.97
TP	531	0.00	5.00	2.69	1.42
TU	531	0.00	5.00	2.15	1.20
TS	531	0.00	5.00	2.47	1.12
TE	531	0.00	5.00	1.89	1.13
Valid N (listwise)	531				

APPENDIX G

FULL SURVERY ADMINSTRATION RESPONSES AND FREQUENCIES

Background Information

001 Please choose the interval below which includes your age...

	below 19	19 - 24	25 - 29	30 - 34	35 - 39	40 - 44	45 - 49	50 - 54	55 - 59	60 - 64	over 64
% of responses	0	2	9	11	16	11	15	16	15	2	3

002 Please indicate your gender...

	female	male
% of responses	51	49

003 Please select the range which best indicates your level of education...

	< HSG	HSG	TS	<CG	CG	<GD	1st GD	2nd GD
% of responses	0	3	2	11	19	7	28	30

004 Please select the range which best indicates your years of computer use...

% of responses	< 1	1 - 3	4 - 6	7 - 10	11 - 13	14 - 16	17 - 20	21 - 25	26 - 30	> 30
	0	1	1	7	7	17	27	20	11	8

005a Please indicate your current job classification...

	Staff	A/P	NTF	Faculty
% of responses	23	41	10	25

005b Please indicate your current university area...

	Admin	Agri	AAES	ACES	Arch	Bus	Ed	Eng	Forestry
% of responses	23	6	2	14	0	6	2	11	1

	Grad Sch	Honors	Hum Sci	Lib Art	Nursing	Outreach	Pharm	COSAM	VetMed
% of responses	1	0	2	5	2	4	3	9	9

On-campus Information Technology

006 Please select a range to estimate your average weekly hours of on-campus computer use...

	none	< 1	1 - 5	6 - 10	11 - 15	16 - 20	21 - 25	26 - 30	31 - 35	36 - 40	> 40
% of responses	7	1	2	3	11	10	16	14	10	19	7

007 Please identify the operating system (OS) on your main on-campus computer...

	DOS	Linux	Mac	WIN 3.1	WIN 95	WIN 98	WIN NT	WIN 2000	WIN ME	WIN XP	Do not know	Not applicable
% of responses	0	1	5	0	0	1	1	5	1	79	1	7

008 Please identify the type of local-area-network (LAN) connection for your main on-campus computer...

	do not know	none	hub router	wireless router combo
% of responses	61	5	25	9

009 Please identify the type of Internet connection for your main on-campus computer...

	do not know	not applicable	dial up	wired	wireless
% of responses	23	8	1	60	8

010 Please select a range to estimate your average weekly hours of on-campus Internet use...

	N/A	none	< 1	1 - 5	6 - 10	11 - 15	16 - 20	21 - 25	26 - 30	31 - 35	36 - 40	> 40
% of responses	5	2	14	40	16	9	5	2	2	1	3	1

011 Please check all the on-campus computer locations that you use...

Type --------------->	none	office	RESNET	library	OIT labs	college labs	school labs	Dept. labs	other labs
% of responses	2	94	2	44	11	35	23	21	5

Number------------>	0	1	2	3	4	5	6	7
% of responses	2	39	12	27	11	6	2	1

Off-campus Information Technology

012 Please select a range to estimate your average weekly hours of off-campus computer use...

	none	< 1	1 - 5	6 - 10	11 - 15	16 - 20	21 - 25	26 - 30	31 - 35	36 - 40	> 40
% of responses	2	6	25	28	13	10	6	6	1	2	1

013 Please identify the operating system (OS) on your main off-campus computer...

	Do not know	Not applicable	DOS	Linux	Mac	WIN 3.1	WIN 95	WIN 98	WIN NT	WIN 2000	WIN ME	WIN XP
% of responses	2	3	0	1	2	0	1	5	1	6	4	76

014 Please identify the type of local-area-network (LAN) connection for your main off-campus computer...

	do not know	none	hub router	wireless router combo
% of responses	21	18	21	40

015 Please identify the type of Internet connection for your main off-campus computer...

	N/A	do not	none	Dial-up	DSL	Cable	Satellite
% of responses	3	3	2	11	20	60	1

016 Please select a range to estimate your average weekly hours of off-campus Internet use...

	none	< 1	1 - 5	6 - 10	11 - 15	16 - 20	21 - 25	26 - 30	31 - 35	36 - 40	> 40
% of responses	4	7	28	30	11	8	5	2	1	2	1

Security Software Installation (alpha = 0.95)

To what extent do you agree with the following statements: (each statement requires a response) % of responses

In my opinion, I could install and set up security software...	Average	not at all	to a small extent	average extent	to a large extent	with out question
017 ...if there were no one around to tell me what to do as I go.	3.12	12.6	21.5	24.3	24.9	16.8
018 ...if I had never used another application like it before.	2.95	14.7	24.1	25.4	22.8	13.0
019 ...if I had only manuals for reference.	3.48	3.8	17.7	27.9	28.4	22.2
020 ...if I had seen someone else set it up before trying it myself.	3.68	3.8	11.5	24.7	33.1	26.9
021 ...if I could call someone for help if I got stuck.	3.97	1.9	7.5	20.9	30.7	39.0
022 ...if someone else helped me get started.	3.94	2.6	7.2	18.8	36.3	35.0
023 ...if I had a lot of time for the completion of the task(s).	3.79	2.8	9.2	24.9	31.8	31.3
024 ...if I had only the built-in help facility for assistance.	3.45	5.8	15.8	28.2	28.1	22.0
025 ...if someone showed me how to do it first.	4.13	2.1	5.5	16.8	29.0	46.7
026 ...if I had set up similar applications before to obtain the same goal.	4.08	1.1	7.2	17.1	32.2	42.4

Information Technology Innovativeness (alpha = .84)

To what extent do you agree with the following statements: (each statement requires a response) % of responses

With respect to my approach toward information technology and its security…	Average	not at all	to a small extent	average extent	to a large extent	with out question
027 ...my peers ask me for advice or information.	2.68	19.8	24.7	31.8	15.6	8.1
028 ...I enjoy trying out new ideas.	3.21	5.6	21.3	32.4	27.5	13.2
029 ...I seek out new ways to do things.	3.12	6.8	23.2	32.6	26.6	10.9
030 ...I am generally cautious about accepting new ideas.	2.65	10.0	37.3	34.5	14.5	3.8
031 ...I frequently improvise methods for solving a problem when an answer is not obvious.	3.11	5.6	21.7	36.3	28.6	7.7
032 ...I am suspicious of new ways of thinking.	2.20	23.9	42.7	25.0	6.0	2.3
033 ...I rarely trust new ideas until I can see whether the vast majority of people around me accept them.	2.20	24.1	41.6	25.2	8.5	0.6
034 ...I feel that I am an influential member of my peer group.	3.11	6.2	15.6	46.3	24.5	7.3
035 ...I consider myself to be creative and original in my thinking and behavior.	3.40	3.2	11.1	38.4	36.5	10.7
036 ...I am usually one of the last people in my peer group to accept something new.	1.93	37.5	37.9	20.0	3.4	1.3
037 ...I am an inventive kind of person.	2.80	10.7	27.7	38.6	16.9	6.0
038 ...I enjoy taking part in the leadership responsibilities of groups.	3.14	6.8	20.0	34.7	29.8	8.9
039 ...I am reluctant about adopting new ways of doing things until I see them working for people around me.	2.31	19.4	40.9	30.5	8.1	1.1
040 ... I find it stimulating to be original in my thinking and behavior.	3.35	3.0	15.4	36.0	34.8	10.7
041 ...I tend to feel that the old way of living and doing things is the best way.	2.11	25.4	44.8	24.1	4.5	1.1
042 ...I am challenged by ambiguities and unsolved problems.	3.11	5.3	21.7	38.0	26.9	8.1
043 ...I must see other people using new technologies before I will consider them.	2.21	24.5	40.7	25.8	7.7	1.3
044 ...I am receptive to new ideas and practices.	3.57	1.7	7.3	37.3	39.4	14.3
045 ...I am challenged by unanswered questions.	3.29	3.6	14.5	40.3	33.0	8.7
046 ...I often find myself skeptical of new ideas and practices.	2.28	17.3	48.6	25.2	6.0	2.8

Item-responses that did not load on factor

Response percentage of 20% or higher

Information Security Awareness (alpha = .92)

To what extent do you agree with the following statements: (each statement requires a response) % of responses

With respect to information technology and its security, I am aware...	Average	not at all	to a small extent	average extent	to a large extent	with out question	I do not understand
047 ...that virus protection software can identify and remove known viruses.	4.24	1.3	2.3	11.9	32.4	50.7	1.5
048 ...that virus protection software requires frequent updates.	4.40	0.9	2.3	8.9	24.5	62.0	1.5
049 ...that firewall software can block network attacks.	3.72	1.9	4.7	17.1	32.4	36.0	7.9
050 ...that personal firewall software can block logical port access to/from a computer.	3.03	4.7	9.0	15.8	25.8	26.0	18.6
051 ...that it is a good idea to keep my passwords safeguarded.	4.44	0.6	3.4	8.5	14.9	70.4	2.3
052 ...that the Auburn University virus protection policy requires use of available software and updates	3.60	4.3	6.8	14.3	23.0	41.4	10.2
053 ...that the Auburn University Office of Information Technology offers virtual private network (VPN) software for use outside of the on-campus intranet.	2.40	15.1	12.8	14.3	11.3	22.2	24.3
054 ...that the Auburn University virus protection policy requires the restriction or quarrantine of computes with viruses.	2.79	11.3	12.2	14.7	17.1	26.2	18.5
055 ...that the Auburn University acceptable use policy dictates that wired and wireless network access requires an user-id and password.	3.55	3.6	6.2	13.0	21.5	42.7	13.0
056 ...that other users have suggested that computer viruses can infect emails or email attachments.	4.14	1.3	3.8	11.5	25.0	54.0	4.3
057 ...that as a computer user, my knowledge of computer threats plays a significant role.	3.86	1.3	6.4	19.8	33.9	35.4	3.2
058 ...that a current, restorable data back-up is necessary.	3.80	1.3	7.9	19.2	26.0	40.3	5.3
059 ...that password secrecy is fundamental.	4.34	0.6	2.4	9.8	24.5	60.3	2.4
060 ...of the impact that a virus can have on my computer system.	4.28	0.4	2.3	11.3	27.9	55.6	2.6
061 ...of the impact that spyware or adware can have on my computer system.	3.99	1.3	4.0	14.7	28.6	46.3	5.1
062 ...of the impact network attacks can have on my computer system.	3.79	1.7	7.7	18.5	25.0	41.2	5.8
063 ...of the vulnerability associated with shared devices such as files, drives, or printers.	3.69	3.2	10.0	19.2	23.9	38.6	5.1
064 ...that encryption can deter unauthorized access to sensitive information (i.e. credit card numbers, social security numbers, confidential emails and documents).	3.66	2.3	7.3	16.2	25.6	39.5	9.0
065 ...that software requires periodic decisions and updates.	4.14	0.8	4.3	13.0	28.6	50.3	3.0

"I do not understand question" percentage of 10% or higher

On-campus Information Security Practices (alpha = .88)

To what extent do you agree with the following statements: (each statement requires a response) % of responses

When using on-campus computer systems...	Average	not at all	to a small extent	average extent	to a large extent	with out question	I do not understand
066 ...I log off when I leave a computer system.	4.18	2.8	7.5	8.5	12.4	65.0	3.8
067 ...I shut down and power-off when leaving a computer system.	2.08	46.3	20.3	10.5	7.7	11.7	3.4
068 ...all of my computer sessions require entering a unique user-id and password combination.	4.14	4.1	5.3	9.6	13.6	63.3	4.1
069 ...I back-up my data on reliable media (disks, CDs).	2.84	18.8	19.4	20.0	20.2	17.1	4.5
070 ...I test the restorability of back-up files that I have created.	2.42	32.4	20.7	15.1	12.1	14.9	4.9
071 ...I check that virus protection software is enabled and updated.	2.75	28.1	15.8	14.7	13.7	23.2	4.5
072 ...I rely on university provided virus protection software and its updates.	3.94	7.5	4.1	10.4	20.2	53.3	4.5
073 ...I check for new versions of virus protection software.	2.42	34.8	19.0	15.8	11.3	15.3	3.8
074 ...I review virus protection software logs for scheduled updates and drive scans.	2.05	45.2	18.8	15.1	7.3	9.6	4.0
075 ...personal firewall software monitors network traffic into/out of my computer(s).	2.11	29.4	11.1	13.6	10.7	15.1	20.2
076 ...as I surf the Web, I allow my Web browser to accept cookies from Web sites.	2.28	12.8	17.1	23.7	20.9	5.3	20.2
077 ...as I surf the Web, I allow my Web browser to download software as deemed necessary.	2.36	21.5	24.1	25.0	17.7	4.1	7.5
078 ...I allow software to save user-ids and passwords for faster access on return visits.	1.64	58.0	16.9	9.4	8.9	1.7	5.1
079 ...I remotely connect to other computers and share drives, printers, or files.	1.90	43.7	19.8	14.9	7.7	6.2	7.7
080 ...I use file transfer software to securely move files between computers.	1.81	43.7	14.3	16.9	7.3	5.6	12.1
081 ...I store email on my computer rather than the email server.	1.77	47.5	12.4	11.7	9.6	6.2	12.6
082 ...I open emails regardless of knowing the sender's identity.	1.62	51.6	29.4	8.7	4.0	1.9	4.5
083 ...I encrypt confidential files with passwords.	1.67	46.1	16.4	13.9	4.0	6.0	13.6
084 ...I look for "https://" before I make financial transactions over the Internet.	2.24	32.4	10.7	12.2	9.2	19.2	16.2
085 ...other people share the computer(s) I routinely use that has (have) Internet access.	2.26	35.2	18.1	12.4	10.9	14.7	8.7
086 ...viruses affect the performance of my computer.	2.20	33.0	14.7	11.1	7.3	19.0	14.9
087 ...virus protection software has identified and limited virus impact to my computer.	2.78	10.7	10.5	15.6	17.1	26.2	19.8
088 ...I routinely choose to change my password(s).	2.05	35.4	28.1	21.1	4.9	6.0	4.5
089 ...I use a character sequence like Ij4Gf4Se%f# as my computer password.	2.05	51.2	13.6	12.1	6.6	12.8	3.8

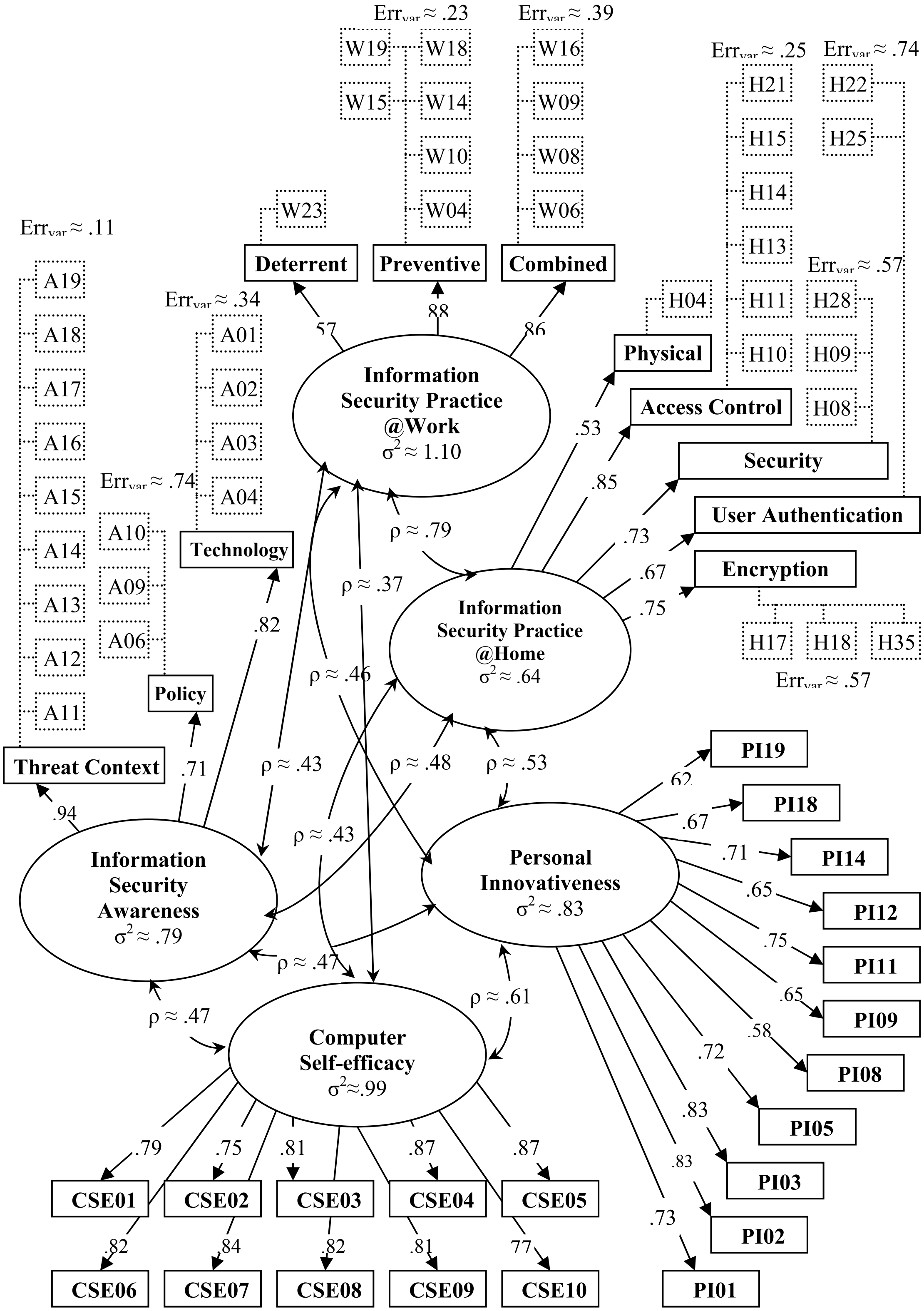
Off-campus Information Security Practices (alpha = .90)

To what extent do you agree with the following statements: (each statement requires a response)

		% of responses					
When using off-campus computer systems...	Average	not at all	to a small extent	average extent	to a large extent	with out question	I do not understand
090 ...I log off when I leave a computer system.	2.85	27.3	16.2	16.8	12.1	25.4	2.3
091 ...I shut down and power off when leaving a computer system.	2.68	28.1	21.7	16.2	10.9	20.9	2.3
092 ...all of my computer sessions require entering a unique user-id and password combination.	2.89	27.5	17.7	13.0	12.8	27.1	1.9
093 ...I back-up my data to reliable media (disks, CDs).	2.69	21.8	26.0	19.2	15.4	15.1	2.4
094 ...I test the restorability of back-up files that I have created.	2.44	32.0	22.8	13.7	12.8	14.7	4.0
095 ...I check that my virus protection software is enabled and updated.	3.44	11.3	11.7	20.7	20.0	33.5	2.8
096 ...I rely on university provided virus protection software.	2.33	44.4	10.4	13.2	7.3	19.8	4.9
097 ...I check for new versions of virus protection software.	3.10	17.5	15.4	20.9	14.1	28.4	3.6
098 ...I review virus protection software logs for scheduled updates and drive scans.	2.65	26.0	19.8	18.5	14.1	17.5	4.1
099 ...personal firewall software monitors traffic into / out of my computer(s).	2.60	17.9	10.9	13.2	13.4	25.4	19.2
100 ...as I surf the Web, I allow my Web browser to accept cookies from Web sites.	2.29	12.1	24.9	26.6	15.6	5.1	15.8
101 ...as I surf the Web, I allow my Web browser to download software as deemed necessary.	2.43	17.1	29.6	27.7	15.4	4.3	5.8
102 ...I remotely connect to other computers and share drives, printers, or files.	1.80	46.7	21.7	15.1	5.6	4.5	6.4
103 ...I use file transfer software to securely move files between computers.	1.87	42.9	17.1	15.4	6.2	7.7	10.5
104 ...I store email on my computer rather than the email server.	1.97	46.5	14.3	11.7	10.0	9.4	8.1
105 ...I open emails regardless of knowing the sender's identity.	1.54	56.5	26.9	8.1	2.8	1.7	4.0
106 ...I encrypt confidential files with passwords.	1.82	43.3	20.7	11.3	7.0	7.2	10.5
107 ...I look for "https://" before I make financial transactions over the Internet.	2.51	29.0	13.7	14.5	10.2	22.0	10.5
108 ...other people share my computer(s) that have Internet access.	2.40	30.5	21.5	16.4	13.0	13.0	5.6
109 ...viruses affect the performance of my computer.	2.43	29.8	18.6	13.7	7.9	20.5	9.4
110 ...virus protection software has identified and limited virus impact to my computer.	3.23	6.4	12.1	19.4	20.3	30.5	11.3
111 ...I routinely choose to change my password(s).	2.08	36.0	29.4	19.2	6.6	5.8	3.0
112 ...I use a surge protector and / or an uninterruptible power supply (UPS).	3.79	8.7	4.9	12.4	13.0	54.2	6.8
113 ...all wired or wireless access to the Internet is password protected.	3.04	16.8	10.5	14.3	11.7	35.2	11.5
114 ...I use a character sequence like Ij4Gf4Se%f# as my computer password.	2.23	46.3	15.8	11.1	7.0	16.8	3.0
115 ...I allow unknown users to access my computer files through the Internet (i.e. music, file sharing, personal Web Server, etc.).	1.57	63.7	14.5	8.9	4.9	3.6	4.5
116 ...I try to use the same password(s) for convenience.	3.10	10.0	22.0	21.3	27.7	16.2	2.8
117 ...I have other email account(s) forwarded to one main email account.	1.67	64.2	12.6	8.7	5.5	6.0	3.0
118 ...I use a spam filter on my email account(s).	3.13	17.1	9.2	16.2	17.3	31.8	8.3
119 ...I have virus protection software on my off-on-campus computer.	4.15	3.8	2.6	12.6	13.6	62.7	4.7
120 ...I have shared devices (files, folders, drives, or printers) that are not password protected or user restricted.	2.04	41.6	12.6	17.9	13.4	6.0	8.5
121 ...I have other computer systems or appliances that share an Internet connection.	2.07	43.5	11.9	16.0	10.0	10.4	8.3
122 ...I have a personal firewall on my off-on-campus computer.	2.83	16.9	6.4	12.4	9.6	35.6	19.0
123 ...other people know my password(s).	1.62	51.6	30.3	8.5	2.6	2.8	4.1
124 ...I use virtual private network (VPN) software to access other computers or other computer networks.	1.35	42.2	10.0	9.0	4.1	5.8	28.8
125 ...I turn off or disconnect my Internet connection(s) when not in use.	2.55	37.1	13.7	12.8	9.6	22.8	4.0
126 ...I share information security concerns with other people that share my computer systems or Internet access.	2.40	29.9	18.6	17.9	11.1	14.9	7.5

APPENDIX H

CONFIRMATORY FACTOR ANALYSIS (CFA) MODEL


Errvar ≈ .23
Errvar ≈ .39
W19
W18
W16
W15
W14
W09
W10
W08
W04
W06
W23
Errvar ≈ .25
Errvar ≈ .74
H21
H22
H15
H25
H14
H13
Errvar ≈ .11
Deterrent
Preventive
Combined
Errvar ≈ .57
H04
H11
H28
H10
H09
H08
Errvar ≈ .34
A19
A18
A01
A17
A02
A16
A03
A15
A04
A14
A13
A12
A11
Errvar ≈ .74
A10
A09
A06
Technology
Policy
Threat Context
.57
.88
.86
Information Security Practice @Work σ² ≈ 1.10
Physical
Access Control
Security
User Authentication
Encryption
.53
.85
.73
.67
.75
ρ ≈ .79
ρ ≈ .37
Information Security Practice @Home σ² ≈ .64
H17
H18
H35
Errvar ≈ .57
.82
ρ ≈ .46
.71
.94
ρ ≈ .43
ρ ≈ .48
ρ ≈ .53
PI19
PI18
PI14
PI12
PI11
PI09
PI08
PI05
PI03
PI02
PI01
.62
.67
.71
.65
.75
.65
.58
.72
.83
.83
.73
ρ ≈ .43
Information Security Awareness σ² ≈ .79
Personal Innovativeness σ² ≈ .83
ρ ≈ .47
ρ ≈ .61
ρ ≈ .47
Computer Self-efficacy σ²≈.99
.79
.75
.81
.87
.87
CSE01
CSE02
CSE03
CSE04
CSE05
.82
.84
.82
.81
.77
CSE06
CSE07
CSE08
CSE09
CSE10

APPENDIX I

AWARENESS AND PRACTICE ASSOCIATIONS

Within ISA Associations (p<.05):

squared correlation (r^2) **large effect** **medium effect** small effect
p-value

	A01	A02	A03	A04	A06	A09	A10	A11	A12	A13	A14	A15	A16	A17	A18	A19
A01		**0.66**	**0.26**	**0.09**	**0.13**	0.08	**0.21**	**0.12**	**0.11**	**0.20**	**0.20**	**0.12**	**0.10**	0.08	**0.09**	**0.19**
		0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
A02	0.66		**0.25**	**0.09**	**0.14**	**0.10**	**0.30**	**0.19**	**0.16**	**0.27**	**0.25**	**0.17**	**0.13**	**0.13**	**0.11**	**0.29**
	0.00		0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
A03	0.26	0.25		**0.37**	**0.16**	**0.12**	**0.14**	**0.10**	**0.14**	**0.13**	**0.12**	**0.13**	**0.23**	**0.12**	**0.18**	**0.15**
	0.00	0.00		0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
A04	0.09	0.09	0.37		**0.15**	**0.17**	**0.10**	0.06	0.06	0.04	0.06	**0.14**	**0.18**	**0.15**	**0.15**	0.07
	0.00	0.00	0.00		0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
A06	0.13	0.14	0.16	0.15		**0.20**	**0.17**	**0.11**	**0.18**	**0.12**	**0.11**	**0.12**	**0.22**	**0.21**	**0.15**	**0.16**
	0.00	0.00	0.00	0.00		0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
A09	0.08	0.10	0.12	0.17	0.20		**0.29**	**0.10**	**0.13**	**0.09**	**0.10**	**0.14**	**0.15**	**0.11**	**0.13**	**0.10**
	0.00	0.00	0.00	0.00	0.00		0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
A10	0.21	0.30	0.14	0.10	0.17	0.29		**0.16**	**0.13**	**0.23**	**0.23**	**0.16**	**0.16**	**0.15**	**0.18**	**0.23**
	0.00	0.00	0.00	0.00	0.00	0.00		0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
A11	0.12	0.19	0.10	0.06	0.11	0.10	0.16		**0.25**	**0.24**	**0.24**	**0.12**	**0.20**	**0.22**	**0.12**	**0.19**
	0.00	0.00	0.00	0.00	0.00	0.00	0.00		0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
A12	0.11	0.16	0.14	0.06	0.18	0.13	0.13	0.25		**0.30**	**0.20**	**0.10**	**0.23**	**0.24**	**0.27**	**0.23**
	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00		0.00	0.00	0.00	0.00	0.00	0.00	0.00
A13	0.20	0.27	0.13	0.04	0.12	0.09	0.23	0.24	0.30		**0.51**	**0.27**	**0.19**	**0.25**	**0.23**	**0.35**
	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00		0.00	0.00	0.00	0.00	0.00	0.00
A14	0.20	0.25	0.12	0.06	0.11	0.10	0.23	0.24	0.20	0.51		**0.49**	**0.30**	**0.28**	**0.17**	**0.35**
	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00		0.00	0.00	0.00	0.00	0.00
A15	0.12	0.17	0.13	0.14	0.12	0.14	0.16	0.12	0.10	0.27	0.49		**0.33**	**0.27**	**0.11**	**0.21**
	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00		0.00	0.00	0.00	0.00
A16	0.10	0.13	0.23	0.18	0.22	0.15	0.16	0.20	0.23	0.19	0.30	0.33		**0.42**	**0.21**	**0.30**
	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00		0.00	0.00	0.00
A17	0.08	0.13	0.12	0.15	0.21	0.11	0.15	0.22	0.24	0.25	0.28	0.27	0.42		**0.28**	**0.30**
	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00		0.00	0.00
A18	0.09	0.11	0.18	0.15	0.15	0.13	0.18	0.12	0.27	0.23	0.17	0.11	0.21	0.28		**0.29**
	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00		0.00
A19	0.19	0.29	0.15	0.07	0.16	0.10	0.23	0.19	0.23	0.35	0.35	0.21	0.30	0.30	0.29	
	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	

Within ISP@W Associations (p<.05):

squared correlation (r^2) **large effect** **medium effect** small effect
p-value

	W04	**W06**	**W08**	**W09**	**W10**	**W14**	**W15**	**W16**	**W18**	**W19**	**W23**
W04		**0.18**	**0.18**	**0.21**	**0.12**	0.08	**0.16**	0.08	**0.09**	0.04	**0.11**
		0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
W06	0.18		**0.59**	**0.45**	**0.27**	**0.10**	**0.17**	**0.17**	**0.12**	**0.12**	**0.19**
	0.00		0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
W08	0.18	0.59		**0.58**	**0.31**	**0.12**	**0.19**	**0.13**	**0.13**	**0.12**	**0.21**
	0.00	0.00		0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
W09	0.21	0.45	0.58		**0.37**	**0.10**	**0.19**	**0.16**	**0.14**	**0.12**	**0.20**
	0.00	0.00	0.00		0.00	0.00	0.00	0.00	0.00	0.00	0.00
W10	0.12	0.27	0.31	0.37		0.07	**0.15**	0.07	**0.12**	0.08	0.09
	0.00	0.00	0.00	0.00		0.00	0.00	0.00	0.00	0.00	0.00
W14	0.08	0.10	0.12	0.10	0.07		**0.30**	0.09	**0.11**	**0.11**	0.09
	0.00	0.00	0.00	0.00	0.00		0.00	0.00	0.00	0.00	0.00
W15	0.16	0.17	0.19	0.19	0.15	0.30		**0.18**	**0.16**	**0.11**	0.08
	0.00	0.00	0.00	0.00	0.00	0.00		0.00	0.00	0.00	0.00
W16	0.08	0.17	0.13	0.16	0.07	0.09	0.18		**0.09**	0.07	**0.09**
	0.00	0.00	0.00	0.00	0.00	0.00	0.00		0.00	0.00	0.00
W18	0.09	0.12	0.13	0.14	0.12	0.11	0.16	0.09		**0.17**	**0.16**
	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00		0.00	0.00
W19	0.04	0.12	0.12	0.12	0.08	0.11	0.11	0.07	0.17		**0.16**
	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00		0.00
W23	0.11	0.19	0.21	0.20	0.09	0.09	0.08	0.09	0.16	0.16	
	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	

Within ISP@H Associations (p<.05):

squared correlation (r^2) **large effect** **medium effect** small effect
p-value

	H04	H08	H09	H10	H11	H13	H14	H15	H17	H18	H21	H22	H25	H28	H35
H04		**0.14**	**0.13**	**0.10**	0.05	0.07	**0.10**	0.06	**0.15**	**0.15**	0.05	**0.15**	0.07	0.04	0.05
		0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
H08	0.14		**0.53**	**0.37**	**0.10**	0.05	**0.09**	0.04	0.05	**0.16**	**0.24**	**0.12**	0.04	0.04	0.06
	0.00		0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
H09	0.13	0.53		**0.33**	0.07	0.06	0.07	0.03	0.07	**0.10**	**0.15**	**0.13**	0.06	0.04	0.04
	0.00	0.00		0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
H10	0.10	0.37	0.33		**0.12**	0.08	**0.10**	0.04	0.08	**0.10**	**0.14**	**0.12**	0.06	0.05	**0.12**
	0.00	0.00	0.00		0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
H11	0.05	0.10	0.07	0.12		**0.15**	**0.13**	0.08	**0.11**	**0.14**	0.06	0.06	0.05	0.07	**0.10**
	0.00	0.00	0.00	0.00		0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
H13	0.07	0.05	0.06	0.08	0.15		**0.32**	0.05	**0.15**	0.06	0.03	0.04	0.04	**0.13**	**0.14**
	0.00	0.00	0.00	0.00	0.00		0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
H14	0.10	0.09	0.07	0.10	0.13	0.32		0.08	**0.25**	**0.16**	0.06	**0.09**	0.08	**0.14**	**0.21**
	0.00	0.00	0.00	0.00	0.00	0.00		0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
H15	0.06	0.04	0.03	0.04	0.08	0.05	0.08		0.07	0.08	0.03	0.03		0.08	0.07
	0.00	0.00	0.00	0.00	0.00	0.00	0.00		0.00	0.00	0.00	0.00		0.00	0.00
H17	0.15	0.05	0.07	0.08	0.11	0.15	0.25	0.07		**0.17**	0.03	**0.17**	**0.09**	0.06	**0.12**
	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00		0.00	0.00	0.00	0.00	0.00	0.00
H18	0.15	0.16	0.10	0.10	0.14	0.06	0.16	0.08	0.17		0.08	**0.16**	**0.09**	0.07	0.08
	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00		0.00	0.00	0.00	0.00	0.00
H21	0.05	0.24	0.15	0.14	0.06	0.03	0.06	0.03	0.03	0.08		**0.13**	0.05	0.04	0.03
	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00		0.00	0.00	0.00	0.00
H22	0.15	0.12	0.13	0.12	0.06	0.04	0.09	0.03	0.17	0.16	0.13		**0.26**	0.08	0.08
	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00		0.00	0.00	0.00
H25	0.07	0.04	0.06	0.06	0.05	0.04	0.08		0.09	0.09	0.05	0.26		0.06	**0.12**
	0.00	0.00	0.00	0.00	0.00	0.00	0.00		0.00	0.00	0.00	0.00		0.00	0.00
H28	0.04	0.04	0.04	0.05	0.07	0.13	0.14	0.08	0.06	0.07	0.04	0.08	0.06		**0.17**
	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00		0.00
H35	0.05	0.06	0.04	0.12	0.10	0.14	0.21	0.07	0.12	0.08	0.03	0.08	0.12	0.17	
	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	

ISA-to-ISP@W Associations (p<.05):

squared correlation (r^2) **large effect** **medium effect** small effect
p-value

	W04	W06	W08	W09	W10	W14	W15	W16	W18	W19	W23
A01		0.02								0.02	
		0.00								0.00	
A02		0.03	0.02							0.02	
		0.00	0.00							0.00	
A03	0.02	**0.10**	0.07	0.05	0.08	0.03	0.03	0.02	0.04	0.05	0.03
	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
A04		0.06	0.04	0.05	**0.13**	0.05	0.05	0.03	0.06	0.07	0.05
		0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
A06		**0.09**	0.08	0.06	0.06	0.04	0.04	0.02	0.02	0.05	0.02
		0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
A09		0.07	0.05	0.05	0.06	0.02	0.03	0.03	0.04	0.05	0.03
		0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
A10	0.02	0.06	0.03	0.02	0.03					0.02	
	0.00	0.00	0.00	0.00	0.00					0.00	
A11	0.02	0.05	0.04	0.03	0.03				0.02	0.03	0.03
	0.00	0.00	0.00	0.00	0.00				0.00	0.00	0.00
A12	0.06	**0.09**	0.07	0.05	0.02	0.02	0.06	0.03	0.02	0.06	0.04
	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
A13	0.03	0.05	0.03			0.02			0.02	0.02	0.02
	0.00	0.00	0.00			0.00			0.00	0.00	0.00
A14		0.05	0.02								
		0.00	0.00								
A15		0.04	0.03	0.02	0.03	0.01	0.02	0.01	0.03	0.03	
		0.00	0.00	0.00	0.00	0.05	0.00	0.02	0.00	0.00	
A16	0.04	**0.10**	**0.09**	0.06	0.07	0.04	0.06	0.03	0.07	0.07	0.04
	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
A17	0.05	**0.11**	**0.11**	0.06	0.07	0.03	0.06	0.02	0.06	0.02	0.03
	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
A18	0.07	**0.13**	**0.10**	**0.09**	**0.09**	0.04	0.08	0.04	0.08	0.05	0.05
	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
A19	0.04	**0.11**	0.06	0.04	0.05	0.02	0.03	0.02	0.04	0.03	0.05
	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00

ISA-to-ISP@H Associations (p<.05):

squared correlation (r^2) **large effect** **medium effect** small effect
p-value

	H04	H08	H09	H10	H11	H13	H14	H15	H17	H18	H21	H22	H25	H28	H35
A01		0.06	0.03	0.03	0.02					0.02	0.08				
		0.00	0.00	0.00	0.00					0.00	0.00				
A02		0.10	0.03	0.04	0.02					0.02	0.08				
		0.00	0.00	0.00	0.00					0.00	0.00				
A03	0.04	0.12	0.06	0.12	0.08	0.02	0.04	0.03	0.03	0.06	0.05	0.04	0.04		0.03
	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00		0.00
A04	0.02	0.13	0.11	0.19	0.12	0.03	0.09	0.03	0.05	0.08	0.04	0.06	0.03	0.05	0.10
	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
A06		0.02		0.02	0.02		0.03	0.02		0.07	0.05		0.02	0.02	0.04
		0.00		0.00	0.00		0.00	0.00		0.00	0.00		0.00	0.00	0.00
A09	0.03	0.07	0.06	0.07	0.04		0.04		0.06	0.08	0.05	0.05	0.07		0.04
	0.00	0.00	0.00	0.00	0.00		0.00		0.00	0.00	0.00	0.00	0.00		0.00
A10		0.09	0.03	0.05	0.02		0.02			0.03	0.06				
		0.00	0.00	0.00	0.00		0.00			0.00	0.00				
A11	0.02	0.08	0.04	0.04	0.02		0.03			0.03	0.08	0.04	0.04		
	0.00	0.00	0.00	0.00	0.00		0.00			0.00	0.00	0.00	0.00		
A12	0.06	0.03	0.02	0.02	0.03		0.03		0.02	0.06	0.02	0.02	0.05		0.02
	0.00	0.00	0.00	0.00	0.00		0.00		0.00	0.00	0.00	0.00	0.00		0.00
A13	0.03	0.04			0.03				0.02	0.03	0.03		0.02		
	0.00	0.00			0.00				0.00	0.00	0.00		0.00		
A14	0.02	0.07	0.04	0.03						0.02	0.06	0.03	0.03		
	0.00	0.00	0.00	0.00						0.00	0.00	0.00	0.00		
A15	0.02	0.12	0.09	0.06	0.03		0.04		0.04	0.06	0.10	0.04	0.02		
	0.00	0.00	0.00	0.00	0.00		0.00		0.00	0.00	0.00	0.00	0.00		
A16	0.04	0.09	0.06	0.08	0.04		0.04	0.03	0.03	0.09	0.07	0.06	0.07	0.02	0.05
	0.00	0.00	0.00	0.00	0.00		0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
A17	0.03	0.11	0.07	0.09	0.03		0.06	0.02	0.06	0.05	0.05	0.04	0.05	0.03	0.06
	0.00	0.00	0.00	0.00	0.00		0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
A18	0.04	0.07	0.05	0.07	0.06		0.07	0.02	0.07	0.07	0.05	0.04	0.05	0.03	0.08
	0.00	0.00	0.00	0.00	0.00		0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
A19	0.05	0.10	0.03	0.06	0.03		0.03		0.03	0.05	0.08	0.06	0.05		0.02
	0.00	0.00	0.00	0.00	0.00		0.00		0.00	0.00	0.00	0.00	0.00		0.00

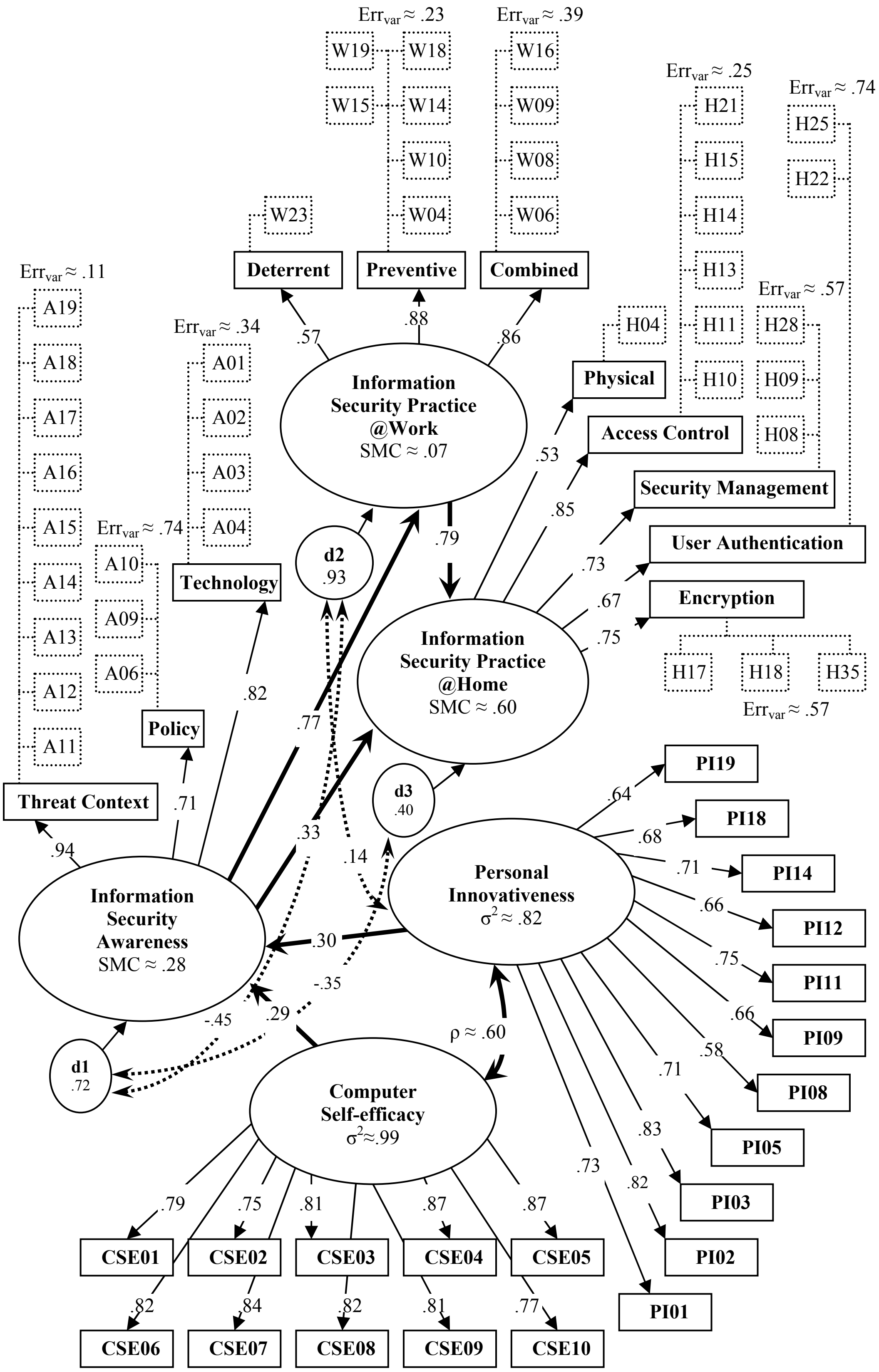
ISP@W-to-ISP@H Associations (p<.05):

squared correlation (r^2) **large effect** **medium effect** small effect
p-value

	H04	**H08**	**H09**	**H10**	**H11**	**H13**	**H14**	**H15**	**H17**	**H18**	**H21**	**H22**	**H25**	**H28**	**H35**
W04	**0.25**	0.05	0.04	0.07	0.02	0.02	0.07	0.04	0.04	0.05		0.04		0.03	0.08
	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00		0.00		0.00	0.00
W06	0.07	0.15	0.07	0.12	0.04		0.07	0.04	0.05	0.08	0.05	0.09	0.08	0.03	0.13
	0.00	0.00	0.00	0.00	0.00		0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
W08	0.09	0.18	0.08	0.08	0.03	0.03	0.08	0.03	0.06	0.08	0.02	0.11	0.07	0.05	0.16
	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
W09	0.11	0.15	0.19	0.10	0.03	0.05	0.13	0.03	0.07	0.08	0.02	0.12	0.09	0.06	0.15
	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
W10	0.07	0.15	0.11	**0.26**	0.04	0.05	0.15	0.02	0.08	0.06	0.07	0.10	0.08	0.07	0.13
	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
W14	0.03	0.03	0.02	0.04	0.10	0.15	0.13	0.04	0.07	0.07	0.02	0.03	0.04	0.07	0.14
	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
W15	0.07	0.03	0.02	0.07	0.08	0.14	**0.44**	0.06	0.15	0.09		0.06	0.05	0.10	**0.25**
	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00		0.00	0.00	0.00	0.00
W16	0.02	0.03	0.02	0.03	0.05	0.03	0.07	**0.26**	0.06	0.07		0.05	0.06	0.08	0.11
	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00		0.00	0.00	0.00	0.00
W18	0.08	0.09	0.08	0.10	0.05	0.07	0.12	0.05	**0.39**	0.10	0.06	0.15	0.08	0.05	0.11
	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
W19	0.07	0.14	0.08	0.09	0.06	0.03	0.09	0.04	0.10	**0.60**	0.06	0.12	0.06	0.06	0.07
	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
W23	0.07	0.06	0.06	0.09	0.03		0.04	0.04	0.06	0.12	0.05	**0.36**	0.11	0.04	0.09
	0.00	0.00	0.00	0.00	0.00		0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00

APPENDIX J

STRUCTURAL EQUATION MODELING (SEM) HYBRID PATH MODEL



Err$_{var}$ ≈ .23
W19
W18
W15
W14
W10
W04
Err$_{var}$ ≈ .39
W16
W09
W08
W06
W23
Deterrent
Preventive
Combined
Err$_{var}$ ≈ .25
H21
H15
H14
H13
H11
H10
Err$_{var}$ ≈ .74
H25
H22
Err$_{var}$ ≈ .57
H28
H09
H08
H04
Physical
Access Control
Security Management
User Authentication
Encryption
H17
H18
H35
Err$_{var}$ ≈ .57
Err$_{var}$ ≈ .11
A19
A18
A17
A16
A15
A14
A13
A12
A11
Err$_{var}$ ≈ .34
A01
A02
A03
A04
Err$_{var}$ ≈ .74
A10
A09
A06
Technology
Policy
Threat Context
.57
.88
.86
Information Security Practice @Work SMC ≈ .07
d2 .93
.79
.53
.85
.73
.67
.75
Information Security Practice @Home SMC ≈ .60
.82
.77
.71
.33
.14
.94
d3 .40
Information Security Awareness SMC ≈ .28
Personal Innovativeness σ^2 ≈ .82
.30
-.35
-.45
.29
d1 .72
ρ ≈ .60
Computer Self-efficacy σ^2≈.99
.64
PI19
.68
PI18
.71
PI14
.66
PI12
.75
PI11
.66
PI09
.58
PI08
.71
PI05
.83
PI03
.73
.82
PI02
PI01
.79
.75
.81
.87
.87
CSE01
CSE02
CSE03
CSE04
CSE05
.82
.84
.82
.81
.77
CSE06
CSE07
CSE08
CSE09
CSE10

APPENDIX K

CATEGORICAL VARIABLE KNOWN-GROUPS AND FREQUENCIES

Individual Demographics:

Age

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	19 -24	12	2.3	2.3	2.3
	25 - 29	46	8.7	8.7	10.9
	30 - 34	58	10.9	10.9	21.8
	35 - 39	84	15.8	15.8	37.7
	40 - 44	64	12.1	12.1	49.7
	45 - 49	79	14.9	14.9	64.6
	50 - 54	83	15.6	15.6	80.2
	55 - 59	80	15.1	15.1	95.3
	60 - 64	11	2.1	2.1	97.4
	over 64	14	2.6	2.6	100.0
	Total	531	100.0	100.0	

Age^

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Below 40 yrs	200	37.7	37.7	37.7
	40 - 49 yrs	143	26.9	26.9	64.6
	50 yrs and above	188	35.4	35.4	100.0
	Total	531	100.0	100.0	

Education Level

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	High School Graduate	14	2.6	2.6	2.6
	Technical School Graduate	9	1.7	1.7	4.3
	Some College	59	11.1	11.1	15.4
	College Graduate	103	19.4	19.4	34.8
	Some Graduate School	37	7.0	7.0	41.8
	1st Graduate Degree	151	28.4	28.4	70.2
	2nd Graduate Degree	158	29.8	29.8	100.0
	Total	531	100.0	100.0	

Education Level^

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	0 Graduate Degree	222	41.8	41.8	41.8
	1 Graduate Degree	151	28.4	28.4	70.2
	2 Graduate Degrees	158	29.8	29.8	100.0
	Total	531	100.0	100.0	

Years of Computer Use

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1 - 3	5	.9	.9	.9
	4 - 6	7	1.3	1.3	2.3
	7 - 10	39	7.3	7.3	9.6
	11 - 13	39	7.3	7.3	16.9
	14 - 16	88	16.6	16.6	33.5
	17 - 20	145	27.3	27.3	60.8
	21 - 25	107	20.2	20.2	81.0
	9	58	10.9	10.9	91.9
	10	43	8.1	8.1	100.0
	Total	531	100.0	100.0	

Years of Computer Use^

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	16 yrs or less	178	33.5	33.5	33.5
	17 - 20 yrs	145	27.3	27.3	60.8
	21 yrs or more	208	39.2	39.2	100.0
	Total	531	100.0	100.0	

Gender

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Female	272	51.2	51.2	51.2
	Male	259	48.8	48.8	100.0
	Total	531	100.0	100.0	

Organizational Demographics:

University Area

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Administration	123	23.2	23.2	23.2
	College of Agriculture	34	6.4	6.4	29.6
	AAES	8	1.5	1.5	31.1
	ACES	74	13.9	13.9	45.0
	College of Business	33	6.2	6.2	51.2
	College of Education	10	1.9	1.9	53.1
	Engineering	61	11.5	11.5	64.6
	School of Forestry & Wildlife	4	.8	.8	65.3
	Graduate School	7	1.3	1.3	66.7
	College of Human Sciences	8	1.5	1.5	68.2
	College of Liberal Arts	29	5.5	5.5	73.6
	School of Nursing	10	1.9	1.9	75.5
	Outreach	19	3.6	3.6	79.1
	School of Pharmacy	16	3.0	3.0	82.1
	College of Science & Mathematics	46	8.7	8.7	90.8
	College of Veterinary Medicine	49	9.2	9.2	100.0
	Total	531	100.0	100.0	

Job Type

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Staff	124	23.4	23.4	23.4
	Academic / Professional	220	41.4	41.4	64.8
	Non-tenure Faculty	53	10.0	10.0	74.8
	Faculty	134	25.2	25.2	100.0
	Total	531	100.0	100.0	

Formal (Business) Technology:

Weekly Hours of Business Computer Use

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	none	38	7.2	7.2	7.2
	less than 1 hour	4	.8	.8	7.9
	1 - 5	13	2.4	2.4	10.4
	6 - 10	17	3.2	3.2	13.6
	11 - 15	61	11.5	11.5	25.0
	16 - 20	51	9.6	9.6	34.7
	21 - 25	87	16.4	16.4	51.0
	26 - 30	73	13.7	13.7	64.8
	31 - 35	51	9.6	9.6	74.4
	36 - 40	99	18.6	18.6	93.0
	greater than 40	37	7.0	7.0	100.0
	Total	531	100.0	100.0	

Weekly Hours of Business Computer Use^

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	20 or less	184	34.7	34.7	34.7
	21 - 30	160	30.1	30.1	64.8
	more than 30	187	35.2	35.2	100.0
	Total	531	100.0	100.0	

Business LAN Type

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Do not know	324	61.0	61.0	61.0
	None	27	5.1	5.1	66.1
	Hub router	133	25.0	25.0	91.1
	Wireless router combo	47	8.9	8.9	100.0
	Total	531	100.0	100.0	

Business Computer OS

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Linux	4	.8	.8	.8
	MAC	25	4.7	4.7	5.5
	W98	5	.9	.9	6.4
	WNT	4	.8	.8	7.2
	W2000	26	4.9	4.9	12.1
	WME	6	1.1	1.1	13.2
	WXP	418	78.7	78.7	91.9
	Do not know	6	1.1	1.1	93.0
	NA	37	7.0	7.0	100.0
	Total	531	100.0	100.0	

Business Internet Connection

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Do not know	124	23.4	23.4	23.4
	NA	42	7.9	7.9	31.3
	Dial up	4	.8	.8	32.0
	Wired	318	59.9	59.9	91.9
	Wireless	43	8.1	8.1	100.0
	Total	531	100.0	100.0	

Business Computer Locations Frequency of Use

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	None	13	2.4	2.4	2.4
	One	206	38.8	38.8	41.2
	Two	62	11.7	11.7	52.9
	Three	144	27.1	27.1	80.0
	Four	57	10.7	10.7	90.8
	Five	34	6.4	6.4	97.2
	Six	12	2.3	2.3	99.4
	Seven	3	.6	.6	100.0
	Total	531	100.0	100.0	

Business Computer Locations

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	None	13	2.4	2.4	2.4
	Office	500	94.2	94.2	96.6
	Library	10	1.9	1.9	98.5
	OIT Labs	2	.4	.4	98.9
	School Labs	1	.2	.2	99.1
	Dept. Labs	5	.9	.9	100.0
	Total	531	100.0	100.0	

Weekly Hours of Business Internet Use

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	not applicable	27	5.1	5.1	5.1
	none	10	1.9	1.9	7.0
	less than 1	74	13.9	13.9	20.9
	1 - 5	214	40.3	40.3	61.2
	6 - 10	84	15.8	15.8	77.0
	11 - 15	48	9.0	9.0	86.1
	16 - 20	27	5.1	5.1	91.1
	21 - 25	11	2.1	2.1	93.2
	26 - 30	13	2.4	2.4	95.7
	31 - 35	4	.8	.8	96.4
	36 - 40	14	2.6	2.6	99.1
	greater than 40	5	.9	.9	100.0
	Total	531	100.0	100.0	

Weekly Hours of Business Internet Use^

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	5 or less	325	61.2	61.2	61.2
	more than 5	206	38.8	38.8	100.0
	Total	531	100.0	100.0	

Informal (Home) Technology:

Weekly Hours of Home Computer Use

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	none	13	2.4	2.4	2.4
	less than 1	32	6.0	6.0	8.5
	1 - 5	131	24.7	24.7	33.1
	6 - 10	147	27.7	27.7	60.8
	11 - 15	70	13.2	13.2	74.0
	16 - 20	54	10.2	10.2	84.2
	21 - 25	30	5.6	5.6	89.8
	26 - 30	32	6.0	6.0	95.9
	31 - 35	5	.9	.9	96.8
	36 - 40	10	1.9	1.9	98.7
	greater than 40	7	1.3	1.3	100.0
	Total	531	100.0	100.0	

Weekly Hours of Home Computer Use^

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	5 or less	176	33.1	33.1	33.1
	6 - 10	147	27.7	27.7	60.8
	more than 10	208	39.2	39.2	100.0
	Total	531	100.0	100.0	

Home Computer OS

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Do not know	12	2.3	2.3	2.3
	NA	16	3.0	3.0	5.3
	Linux	3	.6	.6	5.8
	MAC	10	1.9	1.9	7.7
	W95	5	.9	.9	8.7
	W98	25	4.7	4.7	13.4
	WNT	6	1.1	1.1	14.5
	W2000	32	6.0	6.0	20.5
	WME	19	3.6	3.6	24.1
	WXP	403	75.9	75.9	100.0
	Total	531	100.0	100.0	

Home Comptuer Internet Connection

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	NA	16	3.0	3.0	3.0
	Do not know	15	2.8	2.8	5.8
	None	8	1.5	1.5	7.3
	Dial up	58	10.9	10.9	18.3
	DSL	108	20.3	20.3	38.6
	Cable	319	60.1	60.1	98.7
	Satellite	7	1.3	1.3	100.0
	Total	531	100.0	100.0	

Home Computer Lan Type

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Do not know	111	20.9	20.9	20.9
	None	95	17.9	17.9	38.8
	Hub router	114	21.5	21.5	60.3
	Wireless hub router combo	211	39.7	39.7	100.0
	Total	531	100.0	100.0	

Weekly Hours of Home Internet Use

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	none	20	3.8	3.8	3.8
	less than 1	36	6.8	6.8	10.5
	1 - 5	151	28.4	28.4	39.0
	6 - 10	159	29.9	29.9	68.9
	11 - 15	61	11.5	11.5	80.4
	16 - 20	45	8.5	8.5	88.9
	21 - 25	27	5.1	5.1	94.0
	26 - 30	13	2.4	2.4	96.4
	31 - 35	5	.9	.9	97.4
	36 - 40	9	1.7	1.7	99.1
	greater than 40	5	.9	.9	100.0
	Total	531	100.0	100.0	

Weekly Hours of Home Internet Use^

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	5 or less	207	39.0	39.0	39.0
	6 - 10	159	29.9	29.9	68.9
	more than 10	165	31.1	31.1	100.0
	Total	531	100.0	100.0	