2010

An Investigation of Factors that Affect HIPAA Security Compliance in Academic Medical Centers

James William Brady
Nova Southeastern University, james.brady10@gmail.com

An Investigation of Factors that Affect HIPAA Security Compliance in Academic Medical Centers

by

James W. Brady

A dissertation report submitted in partial fulfillment of the requirements
for the degree of Doctor of Philosophy
in
Information Systems

Graduate School of Computer and Information Sciences
Nova Southeastern University
2010

We hereby certify that this dissertation, submitted by James W. Brady, conforms to acceptable standards and is fully adequate in scope and quality to fulfill the dissertation requirements for the degree of Doctor of Philosophy.

_____ _____

Marlyn Littman, Ph.D. Date
Chairperson of Dissertation Committee

_____ _____

Ling Wang, Ph.D. Date
Dissertation Committee Member

_____ _____

Glenn Stout, Ph.D. Date
Dissertation Committee Member

Approved:

_____ _____

Leonidas Irakliotis, Ph.D. Date
Dean, Graduate School of Computer and Information Sciences

Graduate School of Computer and Information Sciences
Nova Southeastern University

2010

An Abstract of a Dissertation Report Submitted to Nova Southeastern University
in Partial Fulfillment of the Requirements for the Degree of Doctor of Philosophy

An Investigation of Factors that Affect HIPAA Security Compliance in Academic Medical Centers

by
James W. Brady

June 2010

HIPAA security compliance in academic medical centers is a central concern of researchers, academicians, and practitioners. Increased numbers of data security breaches and information technology implementations have caused concern over the confidentiality, integrity, and availability of electronic personal health information. The federal government has implemented stringent HIPAA security compliance reviews and significantly extended the scope and enforcement of the HIPAA Security Rule. However, academic medical centers have shown limited compliance with the HIPAA Security Rule. Therefore, the goal of this study was to investigate the factors that may affect HIPAA security compliance in academic medical centers. Based on a review of the literature of technology acceptance and security effectiveness, this study proposed a theoretical model that uses management support, security awareness, security culture, and computer self-efficacy to predict security behavior and security effectiveness and thus HIPAA security compliance in academic medical centers.

To empirically assess the effect of the above-noted variables on HIPAA security compliance in academic medical centers, a Web-based survey was developed. The survey instrument was designed as a multi-line measure that used Likert-type scales. Previous validated scales were adapted and used in the survey. The sample for this investigation was health care information technology professionals who are members of the Group on Information Resources within the Association of American Medical Colleges.

Two statistical methods were used to derive and validate predictive models: multiple linear regression and correlation analysis. The results of the investigation demonstrated that security awareness, management support, and security culture were significant predictors of both security effectiveness and security behavior. Security awareness was the most significant predictor of security effectiveness and security behavior. Due to the presence of collinearity, Pearson correlation analysis was used to develop a composite factor, consisting of management support and security culture, for the final multiple linear regression model.

By enhancing the understanding of HIPAA security compliance in academic medical centers, the outcomes of this study will contribute to the body of knowledge of security compliance. The empirical results of this research also will provide guidance for

individuals and organizations involved with HIPAA security compliance initiatives in health care.

Acknowledgments

First, I would like to thank the Lord, who is my first love and the one whom I serve. I am very thankful to my dissertation chair, Dr. Marlyn Littman, for her unwavering support, guidance, and patience. Her meticulous review and expertise helped me to formulate the research, making the dream of completing this dissertation possible. I am very grateful for her dedication and generosity in time, effort, and patience. I am profoundly grateful to my committee members, Dr. Ling Wang and Dr. Glenn Stout, for their support, time, and direction. In addition to their guidance as members of my dissertation committee, Dr. Littman, Dr. Wang, and Dr. Stout inspired and influenced me in their courses during my tenure as a graduate student. And finally, to Dr. Scigliano, who as my first Nova Southeastern University professor noted that I would indeed complete the dissertation process.

To my beautiful wife, Jeanne, and my three precious children, Amie, Alisha, and Joshua, I want to thank you for your understanding and support of my educational dream and aspiration. To my parents, particularly my father, a distinguished professor and researcher, thank you for providing me with a wonderful foundation.

Without each and every one of you, I would not be able to achieve the goals that lie before me.

Table of Contents

List of Tables

Tables

Tables (Continued)

List of Figures

Figures

Chapter 1

Introduction

Statement of the Problem

The consensus of the literature is that the identification of the problem is the cornerstone of quality research (Ellis & Levy, 2008). The research problem that the author investigated was that academic medical centers (AMCs) and other covered entities in the U.S. are not fully complying with the Health Insurance Portability and Accountability Act (HIPAA) of 1996 (Hasemyer, 2009; Herold, 2009a; Holland, 2009; Hourihan, 2009). According to Taylor (2006), an AMC is:

> an accredited medical school (including a university, when appropriate); an affiliated faculty practice plan; and one or more affiliated hospital(s) in which a majority of the hospital medical staff consists of physicians who are faculty members and a majority of all hospital admissions are made by physicians who are faculty members. (p. 54)

A covered entity includes every "person, business, or agency that provides, bills or receives payment for medical care and transmits protected health information already saved in electronic storage media" (Lawrence, 2007, p. 430). Based on the results of the 2008 Centers for Medicare & Medicaid Services (CMS) HIPAA security compliance reviews, "covered entities appeared to struggle to comply with the Security Rule" (CMS, Office of E-Health Standards and Services, 2008, p. 2). The overarching compliance issues reported included risk assessment, currency of policies and procedures, security training, workforce clearance, workstation security, and encryption (CMS, Office of E-Health Standards and Services). According to Gallagher (2009), the findings from the

2009 Healthcare Information and Management Systems Society (HIMSS) Security Survey, suggest that:

> despite changes to the security and privacy landscape including new legal and regulatory requirements and increasing risk, health care organizations have made relatively little change since the assessment of the market that HIMSS conducted in 2008 relating to a number of important areas of the security environment. (p. 3)

As indicated by Greenberg and Ridgely (2009), "more than a decade after the passage of HIPAA, concerns about security of patient health information (PHI) remain a major policy issue" (p. 450).

According to Herold (2009b), data security breaches in health care organizations continue to increase. In referencing the University of Utah Hospital data security breach and the results of the 2008 Global State of Information Security Survey, Nash (2008) reported that "information security is, in many ways, failing" (p. 2). Organizations that track security incidents have reported rising numbers of data security breaches involving health care providers, payers, and insurers (Baker et al., 2009; Ernst & Young, 2009; Frost & Sullivan, 2008; Gallagher, 2009; Peters, 2009; Ponemon, 2008; Privacy Rights Clearinghouse, 2010). A large number of security breaches are caused by employees' failure to comply with organizational information security guidelines (Chan, Woon, & Kankanhalli, 2005; Payton, 2006). Further, new security risks and breaches have resulted from the increased use of mobile computing (Fritsche & Rodgers, 2007).

Numerous AMCs reported data security breaches in 2009 and 2010 (DataLossDB, 2010; Privacy Rights Clearinghouse, 2010). Medical schools, teaching hospitals and health systems, and academic and scientific societies are considered members of the

academic medicine community (Association of American Medical Colleges [AAMC], 2009a). Because scientific research involving patients and human volunteers is not regulated under HIPAA, some AMCs have elected to exempt their research activities from HIPAA requirements (AAMC, 2007). As a result, “information security measures protecting human (or animal) research data vary from one AMC (or laboratory) to the next” (AAMC, 2007, p. 3).

According to Helms, Moore, and Ahmadi (2008) and Thomas and Botha (2007), “the slow adoption of information technology (IT)” has been an internal weakness within health care organizations” (p. 75). The health care industry has been viewed as a laggard in terms of technology adoption (Connell & Young, 2007). However, “the use of technology for the communication and storage of medical information has experienced a significant increase over the past several years” (Clarke, Flaherty, Hollis, & Tomallo, 2009, p. 63). According to Clarke et al., this increased communication of health data and storage of electronic medical records has resulted in additional privacy and security risks.

As stated by Nash (2008), health care organizations typically address security requirements reactively. Logan and Noles (2008) noted that such organizations do not always consider security when implementing new products and services. Further, computer security has often been implemented as an afterthought (Ma, Johnston, & Pearson, 2008). Although HIPAA regulations are primarily focused on administrative security controls (Huang, Bai, & Nair, 2008), health care organizations have addressed security issues from a technical viewpoint (Brenner, 2007; Gross & Rosson, 2007). In a study examining the effects of the HIPAA Security Rule on interoperable health information exchanges, Dimitropoulos and Rizk (2009) found that “even though more

than one-third of the rule addresses administrative security requirements, many health care organizations focused disproportionately on technology rather than on administrative safeguards" (p. 430). Health care organizations have sustained losses not because of insufficient or faulty technology, but rather by users of technology and faulty behavior (Rotvold, 2008). Therefore, a combination of administrative and technical control processes is needed to safeguard information and combat security issues (D'Arcy & Hovav, 2009; Jerbic, 2008).

Additionally, shortcomings in the HIPAA Security Rule relating to business associates, breach notifications, data transmission standards, investigation of complaints, and penalties and enforcement have created liabilities for health care organizations (Brown, 2009b). According to Blades (2009), business associates, which include attorneys, third party administrators, state and regional health information exchanges, state and national information networks, personal health record services, data analysts, and billing benefits managers for health care providers, are not subject to regulatory fines and penalties if they violate a HIPAA security requirement. As a result, "vendors have been slow to readily integrate security technologies that can provide improved protection to PHI in transit and at rest" (Brown, 2009a, p. 36).

Drumke (2008) noted that HIPAA does not specify how to securely transmit electronic protected health information (ePHI). In addition, HIPAA protections do not extend to de-identified health information (McGraw, Dempsey, Harris, & Goldman, 2009). As a result, covered entities are allowed to provide de-identified data to third parties for research or business intelligence uses without being subject to the HIPAA requirements (McGraw et al.). As indicated by Hoffman and Podgurski (2007) and Collins (2007), the

HIPAA Security Rule does not allow aggrieved individuals to file suit in court, thus weakening the Security Rule's deterrent power. Further, the HIPAA Security Rule does not mandate reporting of a security breach to patients (Logan & Noles, 2008; Rath, 2009). Moreover, the U.S. Congress has raised concerns that the enforcement of HIPAA security compliance by the U.S. Department of Health and Human Services (HHS) has been weak (Rath).

Literature on HIPAA and information security has identified a number of factors that contribute to security behavior and security effectiveness. These factors include management support (Barry & Grossmeier, 2009; Logan & Noles, 2008; Loghry & Veach, 2009), security awareness (Lending & Dillon, 2007; Medlin & Cazier, 2007; North, North, & North, 2009), security culture (Lineberry, 2007; Ma et al., 2008; Sveen, Rich, & Jager, 2007), and computer self-efficacy (Chan et al., 2005; Lending & Dillon; Womble, 2008). Additionally, security effectiveness (D'Arcy & Hovav, 2009; Hazari, Hargrave, & Clenney, 2008; Jahankhani, Fernando, Nkhoma, & Mouratidis, 2007) and security behavior (Keith, Shao, & Steinbart, 2009; McFadzean, Ezingeard, & Birchall, 2007; Pattinson & Anderson, 2007) were found to be valid predictors of each other as well as of HIPAA security compliance (Chang & Ho, 2006; Johnston & Warkentin, 2008; Rotvold, 2008).

Barry and Grossmeier (2009), Logan and Noles (2008), and Loghry and Veach (2009) view management support as a significant determinant of security compliance. Based on a qualitative investigation into the impact of organizational change on information systems security, Cline, Guynes, and Nyanoga (2010) found that executive management considers security breaches to be a secondary issue, despite their being concerned with

the negative consequences and risks incurred. In an empirical study of 208 health care professionals from 10 health care facilities in the U.S., Johnston and Warkentin (2008) indicated that the likelihood of HIPAA security compliance improved with increased organizational support. However, according to Jahankhani et al. (2007), senior managers failed to view information security as a critical business component. The lack of top management support has resulted in the absence of comprehensive security awareness training programs (Rotvold, 2008). Moreover, Knapp, Marshall, Rainer, and Ford (2006), Ma et al., and McFadzean et al. (2007) reported a lack of executive management support and a lack of understanding of the importance of information security.

Security awareness is a critical factor in attaining HIPAA security compliance (Lending & Dillon, 2007; Medlin & Cazier, 2007; North et al., 2009). Based on a study of 118 employees from five hospitals, Medlin, Cazier, and Foulk (2008) concluded that security awareness training was an important factor in improving HIPAA-compliant password practices. Several other studies have determined that security awareness is lacking (Pfleeger & Rue, 2008; Schmidt, Johnston, Arnett, Chen, & Li, 2008; Sveen et al., 2007). Even when the importance of security awareness exists, "there is a lack of adequate security awareness in practice" (Tsohou, Kokolakis, Karyda, & Kiountouzis, 2008, p. 271).

Security culture plays a significant role in information security management (Lineberry, 2007; Ma et al., 2008; Sveen et al., 2007). According to Chang and Lin (2007), "managers should regard organizational culture as an important factor for supporting and guiding information security management practice" (p. 439). Da Veiga and Eloff (2007) found that it is critical that organizations cultivate "an acceptable level

of information security culture" (p. 371). In a recent study of 32 IT personnel and 89 other employees from eight nonprofit organizations, including a university and hospital, Guzman, Stam, and Stanton (2008) observed that cultural differences were determined to be important in attaining security compliance.

Computer self-efficacy is a significant predictor of security compliance behavior (Chan et al., 2005; Lending & Dillon, 2007; Womble, 2008). Specifically, computer self-efficacy was shown to be important in preventing improper access to personal data (White, Shah, Cook, & Mendez, 2008). In this regard, Johnston and Warkentin (2008) found that "through increased attention and resources dedicated to providing a supportive environment for HIPAA compliance, health care managers increase the likelihood of compliance success by improving employee self-efficacy" (p. 16). Computer self-efficacy was also determined to be a moderator of user security awareness and user response to security countermeasures (D'Arcy & Hovav, 2009).

An effective information security program incorporates a combination of technological and human controls to avoid the loss of information, deter accidental or intentional unauthorized activities, and prevent unauthorized data access (Jahankhani & Nkhoma, 2005). According to D'Arcy and Hovav (2009), Hazari et al. (2008), and Jahankhani et al. (2007), security effectiveness is a valid predictor of security behavior. Hazari et al. noted that effective information security behavior results from organizations understanding social cognitive factors such as attitude, subjective norm, and perceived behavioral control. Further, an effective information security management system has been shown to significantly reduce security breaches (Tang, 2008).

Human behavioral factors have the ability to influence the security of an organization's information systems (Pattinson & Anderson, 2007). Hazari et al. (2008) observed that changing the beliefs, attitudes, and behaviors of individuals and groups led to more enhanced security. Likewise, implementing security training to change staff behavior has been found to increase information security (Filipek, 2007).

Research Goals

The author's goal in conducting this research investigation was to develop and empirically validate a model for predicting the effect of management support, security awareness, security culture, and computer self-efficacy on security behavior and security effectiveness and thus HIPAA security compliance in AMCs. The independent variables were management support (Barry & Grossmeier, 2009; Logan & Noles, 2008; Loghry & Veach, 2009), security awareness (Lending & Dillon, 2007; Medlin & Cazier, 2007; North et al., 2009), security culture (Lineberry, 2007; Ma et al., 2008; Sveen et al., 2007), and computer self-efficacy (Chan et al., 2005; Lending & Dillon, 2007; Womble, 2008). The dependent variables are security behavior (Keith et al., 2009; McFadzean et al., 2007; Pattinson & Anderson, 2007) and security effectiveness (D'Arcy & Hovav, 2009; Hazari et al., 2008; Jahankhani et al., 2007). The conceptual model derived from the findings of this investigation was used to predict intention to comply with the HIPAA Security Rule in lieu of actual HIPAA security compliance. Figure 1 presents the conceptual model for this research, which was developed from the literature.

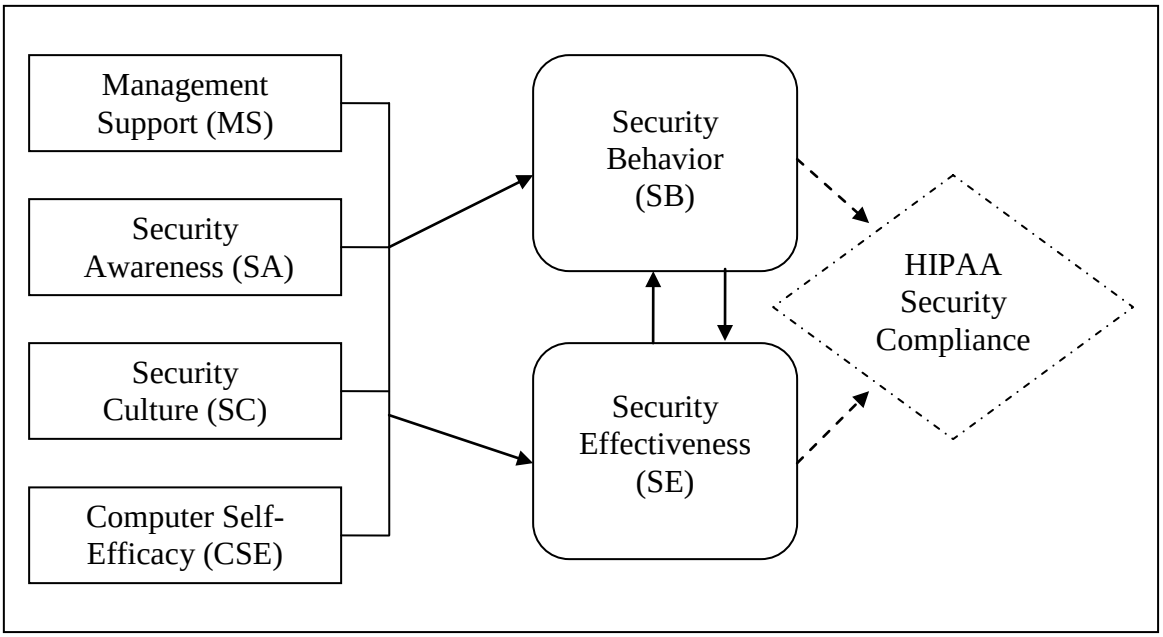

Figure 1. The conceptual model of the relevant factors and their effects on HIPAA security compliance in AMCs.

Relevance and Significance

Need for the Study

The need for this study was sixfold. First, more attention needed to be given to social and behavioral aspects of information security among AMCs (Guzman et al., 2008; Hazari, 2005; Huebner & Britt, 2006; Pattinson & Anderson, 2007). Second, a better understanding of information security effectiveness among AMCs was needed (Chang & Lin, 2007; Knapp et al., 2006; Tsohou et al., 2008). Third, there was a need for greater understanding of management support for information security among AMCs (Da Veiga & Eloff, 2007; Knapp & Boulton, 2006). Fourth, the importance of more computer security awareness, education, and training in the context of AMCs was needed (Aytes & Connolly, 2004; Kruck & Teer, 2008; Wade, 2004). Fifth, more attention needed to be given to the information security culture of AMCs (Da Veiga & Eloff, 2007; Von Solms,

2000). Finally, research on the factors associated with self-efficacy in AMCs was warranted (Ball & Levy, 2008; Lending & Dillon, 2007).

Relevance

The relevance for this study was threefold. First, this investigation was directed to health care professionals within the AAMC (AAMC, 2009a). Based on the findings of this investigation, the author identified the effect of management support, security awareness, security culture, and computer self-efficacy on security behavior and security effectiveness. These findings helped facilitate the understanding of HIPAA security compliance among AMCs (AAMC, 2009b; Lawrence, 2007).

Second, the results of this study provided guidance for the individuals and organizations associated with AMCs, who are involved with HIPAA security compliance initiatives in the health care domain (Helms et al., 2008; Li & Shaw, 2008). The findings of this investigation helped contribute knowledge that can be applied to improve information security and regulatory compliance in the HIPAA domain, with a focus on AMCs.

Third, the research model developed as an outcome of this investigation helped information security researchers and practitioners understand the multiplicity of factors affecting the current HIPAA security requirements as implemented by AMCs (Keith et al., 2009; Ma et al., 2008; Tsohou et al., 2008) as well as the recent HIPAA Security Rule modifications and extensions (Aguilar, 2009; Bianchi, 2009; Maffeo, 2009).

Significance

The significance of this study was fourfold. First, data security breaches have been a continued problem in health care organizations, particularly AMCs, in the U.S. and

globally (Greenberg, & Ridgely, 2009; Gross & Rosson, 2007; Ramanathan, Cohen, Plassmann, & Ramamoorthy, 2007). Second, the increased reliance on IT in health care has created a need for additional security measures ("Responsible information management," 2009; Ross & Chen, 2007; Wyne & Haider, 2007). Third, recent security audits have led to stricter enforcement and improved oversight of the HIPAA Security Rule (Bakhtiari, 2009; Hourihan, 2009; Ruzic, 2009). Finally, new federal regulations and state laws have significantly increased the requirements of the HIPAA Security Rule and the consequences for noncompliance (Bianchi, 2009; Rath, 2009; Swearingen, 2009). Consequently, there was a need to investigate HIPAA security compliance in health care organizations, specifically in AMCs that represent the leading U.S. medical schools, teaching hospitals and health systems, and academic societies (Steinbrook, 2009).

Barriers and Issues

The author identified three potential barriers in conducting this investigation. The first barrier was assuring that an adequate and appropriate sample of AMC representatives completed the survey. To address this barrier, the author chose to use a sample population consisting of health care professionals who have a working knowledge of IT and belong to an organization that supports participation in this research. The second barrier was assuring that the sample population had sufficient knowledge of HIPAA security compliance issues. To address this barrier, the author chose to use a sample population that consisted of health care professionals who regularly address technology and security concerns.

A third barrier was that, due to security and privacy concerns, the sample population might struggle with openly responding to the survey items. According to Kotulic and Clark (2004) and Straub and Welke (1998), the sensitive nature of security as a topic may impede the collection of a sufficient sample willing to participate in the research. Curry and Moore (2003) found that information sharing in the health care environment was often hampered by a perceived need for confidentiality. Other research has noted that the actual occurrence of security issues is often understated (D'Arcy & Hovav, 2009; Logan & Noles, 2008). To address this barrier, the author informed the survey participants that their responses would remain confidential. In addition, the author notified the respondents that the IP address-tracking feature of the Web-based survey software was disabled.

Research Questions

The main research question that this study addressed was: What is the effect of management support, security awareness, security culture, and computer self-efficacy on security behavior and security effectiveness, and thus HIPAA security compliance in AMCs? The main research question can be understood as being comprised of four specific research questions:

1. What is the effect of management support on security behavior and security effectiveness, and thus HIPAA security compliance in AMCs? (Barry & Grossmeier, 2009; Logan & Noles, 2008; Loghry & Veach, 2009).

2. What is the effect of security awareness on security behavior and security effectiveness, and thus HIPAA security compliance in AMCs? (Lending & Dillon, 2007; Medlin & Cazier, 2007; North et al., 2009).

3. What is the effect of security culture on security behavior and security effectiveness, and thus HIPAA security compliance in AMCs? (Lineberry, 2007; Ma et al., 2008; Sveen et al., 2007).

4. What is the effect of computer self-efficacy on security behavior and security effectiveness, and thus HIPAA security compliance in AMCs? (Chan et al., 2005; Lending & Dillon, 2007; Womble, 2008).

Limitations and Delimitations

Limitations

At least three limitations were identified. First, the participants of this study were members of the AAMC, which is an organization comprised of medical schools, teaching hospitals and health systems, and academic and professional societies (AAMC, 2009c). Therefore, the generalizability of this study might be limited only to health care organizations that are considered AMCs. Second, the study was limited by the truthfulness of the respondents. According to Leedy and Ormrod (2005), some respondents "may intentionally misrepresent the facts . . . in order to present a favorable impression to the researcher" (p. 184). Third, the respondents might have encountered difficulties in attempting to remain unbiased while completing the Web-based survey. As a consequence of pre-conceived notions, answers might have followed a particular viewpoint that there were right or wrong answers (Sekaran, 2003).

Delimitations

The literature contains four factors affecting HIPAA security compliance, and, as such, this study was delimited to these constructs, which were the contributions of management support, security awareness, security culture, and computer self-efficacy to security behavior and security effectiveness, and thus HIPAA security compliance in AMCs.

Definition of Terms

The following definitions are provided to ensure a clear understanding of some specific terms used throughout this study.

Academic medical center (AMC):

> An accredited medical school (including a university, when appropriate); an affiliated faculty practice plan; and one or more affiliated hospital(s) in which a majority of the hospital medical staff consists of physicians who are faculty members and a majority of all hospital admissions are made by physicians who are faculty members. (Taylor, 2006, p. 54)

Awareness: The extent to which a target population is conscious of an innovation and formulates a general perception of what it entails (Dinev & Hu, 2007).

Behavioral intention: To perform some specific behavior that is partially determined by attitude toward performing the behavior and that is influenced by beliefs and motivations (Ajzen & Fishbein, 1980). An antecedent of actual behavior, given the right facilitating conditions (Ajzen, 1985).

Climate: The perceived results of organizational policies, practices, and procedures, both formal and informal. More apparent and visible than culture, climate provides researchers with a glimpse of the underlying, less observable culture that resides within the organization (Reichers & Schneider, 1990).

Compliance: "The name given to multi-faceted programs designed to ensure that an organization's culture and collective processes meet legal, regulatory, and ethical requirements" (Gable, 2005, p. 1).

Compliant information security behavior: "The set of core information security activities that need to be carried out by individuals to maintain information security as defined by information security policies" (Chan et al., 2005, p. 22).

Computer self-efficacy (CSE): An individual's perception of one's ability to use a computer to accomplish a particular task. It exerts a significant influence on an individual's actual use of computers, expectations of his or her computer use, and attitude and level of anxiety towards the use of computers. "An individual's judgment of their [sic] computer-related skills in diverse situations" (Compeau & Higgins, 1995, p. 192).

Covered entity (CE): This includes every "person, business, or agency that provides, bills or receives payment for medical care and transmits protected health information already saved in electronic storage media" (Lawrence, 2007, p. 430).

Culture: A phenomenon deeply embedded within the organizational environment and viewed as a deeper, less consciously held set of meanings as compared to climate (Reichers & Schneider 1990).

Encryption: "The use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without the use of a confidential process or key" ("HHS guidance on securing protected health information," 2009, p. 7).

Health care clearinghouse: An entity that processes health information from nonstandard to standard data elements (HIPAA, 2005a).

Health care provider: Any provider of medical or health services, such as a hospital (HIPAA, 2005a).

Health plan: Any individual or group plan that either pays for or provides medical care (HIPAA, 2005a).

Information security:

> A program that allows an organization to protect a continuously interconnected environment from emerging weaknesses, vulnerabilities, attacks, threats, and incidents. The program must address tangibles and intangibles. Information assets are captured in multiple and diverse formats, and policies, processes, and procedures must be created accordingly. (Myler & Broadbent, 2006, p. 44)

Information security awareness: An organizational process aimed at "improving information security by enhancing the adoption of security policies and countermeasures, improving IS users' security behavior, and altering work routine so that good security habits are applied" (Tsohou et al., 2008, p. 272).

Information security governance: "The overall manner in which information security is deployed to mitigate risks" (Da Veiga & Eloff, 2007, p. 362).

Information security policy (ISP): "A policy targeted specifically at improving an organization's information security level" (Hong, Chi, Chao, & Tang, 2006, p. 105). An ISP consists of:

> the rules set-up for the use of information assets, and the statement set-up for the security priorities to achieve organizational objectives; the guideline for the scope of information security; the principle for information management and resource use; and the principle for supporting security techniques. (p. 105)

Information systems security: "Organizational measures taken to protect and control IS resources, so as to reduce the risks and impacts of system vulnerabilities and threats to a level that is considered acceptable by an organization" (Walters, 2007, p. 123).

IS misuse intention: An individual's intention to perform a behavior that is defined by the organization as a misuse of IS resources (Magklaras, Furnell, & Brooke, 2006).

IS security effectiveness: The ability of IS security measures to protect against unauthorized or deliberate misuse of IS assets by people (Straub, 1990).

Intention to use: The intention to use a technology (Levy & Green, 2009).

Organizational climate: A set of attributes specific to a particular organization that may be induced from the way the organization deals with its members and its environment (Campbell, Dunnette, Lawler, & Weick, 1970).

Organizational culture:

> [The] pattern of shared basic assumptions that the group learned as it solved its problems of external adaptations and internal integrations that has 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. (Schein, 1992, p. 12)

"The values, beliefs and assumptions found in the deep structure of organizations, which are held by its members" (Chan et al., 2005, p. 20).

Perceived ease of use: "The extent to which a person believes that using a particular system will be free of effort" (Davis, 1989, p. 320).

Perceived organizational support: Employees' beliefs "concerning the extent to which the organization values their contributions and cares about their well-being" (Rhoades & Eisenberger, 2002, p. 701). The "assurance that aid will be available from the organization . . . to carry out one's job effectively" (Rhoades & Eisenberger, p. 698).

Perceived usefulness: "The extent to which a person believes that using a particular system will enhance his or her performance" (Davis, 1989, p. 320).

Protected health information (PHI): Individually identifiable health information transmitted or maintained in electronic form that is specifically targeted by HIPAA and its security and privacy rules (HIPAA, 2005b).

Protective technologies: Those technologies "that are designed to deter, neutralize, disable, or eliminate the negative technologies or their effectiveness, such as anti-virus software, anti-spyware tools, firewalls, and intrusion detection technologies" (Dinev & Hu, 2007, p. 387).

Risk: "The product of the frequency of some undesirable effect and a measure of its adverse impact" (Baldwin, Beres, Shiu, & Kearney, 2006, p. 61).

Secure behavior intention: A participant's intention to use technology in a secure fashion (Novakovic, McGill, & Dixon, 2009).

Secure usage: A participant's actual usage of technology (Novakovic et al., 2009).

Security: The policies, practices, and technology that must be in place for an organization to transact business electronically via networks with a reasonable assurance of safety (Volonino & Robinson, 2004).

Security culture: "A focus on security in the development of information systems and networks and the adoption of new ways of thinking and behaving when using and interacting within information systems and networks" (Organization for Economic Cooperation and Development, 2002, p. 8).

Security Threat: A threat which creates "circumstances, condition, or event with the potential to cause economic hardship to data or network resources in the form of destruction, disclosure, modification of data, denial of service and/or fraud, waste and abuse" (Kalakota & Whinston, 1997, p. 123).

Self-efficacy: One's beliefs in one's capabilities to successfully perform an explicit area of behavior (Bandura, 1977).

> People's judgments of their capabilities to organize and execute courses of action required to attain designated types of performances. It is concerned, not with the skills one has, but with judgments of what one can do with whatever skills one possesses. (Bandura, 1986, p. 391)

Assesses an individual's belief regarding whether he/she can exercise control over an outcome or not (Bandura & Wood, 1989). "A user's confidence that he or she has the ability to use an information system" (Lending & Dillon, 2007, p. 50).

Social engineering: "The art and science of getting people to comply with your wishes" (Kamal, 2008, p. 145).

Technology awareness: "A user's raised consciousness of an interest in knowing about technological issues and strategies to deal with them" (Dinev & Hu, 2007, p. 391).

Top management support: "The degree that senior management understands the importance of the security function and the extent to which management is perceived supporting security goals and priorities" (Knapp, Marshall, Rainer, & Ford, 2007, p. 52).

Unsecured PHI: "PHI that is not secured through the use of a technology or methodology required in HHS guidance to render PHI unusable, unreadable, or indecipherable to unauthorized individuals" (Dowell, 2009, p. 6).

Summary

This chapter presented the research problem and identified the goals of the study. The research problem that this study investigated was that AMCs in the U.S. have not fully complied with the HIPAA Security Rule. The main goal of this research was to develop and empirically validate a model for predicting the effect of management support, security awareness, security culture, and computer self-efficacy on security behavior and security effectiveness, and thus HIPAA security compliance in AMCs. In addition to the main goal, four specific research goals were identified. Additionally, a conceptual model representing the effect of the four dependent variables on the two independent variables was presented.

The need for the study, along with the relevance and the significance of the study, were presented. Anticipated barriers and issues as well as limitations and delimitations of the study were discussed. The main research question that the study addressed was: What is the effect of management support, security awareness, security culture, and computer

self-efficacy on security behavior and security effectiveness, and thus HIPAA security compliance in AMCs? This investigation also addressed four specific research questions that were generated from the main research question.

Chapter 2

Review of the Literature

Introduction

The author developed a research framework by conducting a literature search in a broad variety of fields, including IS security, sociology and psychology, management science, and organizational behavior to study the factors that affect HIPAA security compliance in AMCs. Table 1 presents a summary of the online databases and keywords that were used to provide the theoretical background for this study.

Table 1. Online Databases and Keywords Used

Online Databases	Keywords Used
ACM Digital Library	HIPAA, security, compliance, effectiveness, behavior, management, awareness, culture, self-efficacy, framework, governance, AMC
IEEE Computer Society Digital Library	HIPAA, security, compliance, effectiveness, behavior, management, awareness, culture, self-efficacy, framework, governance, AMC
ProQuest Computing	HIPAA, security, compliance, effectiveness, behavior, management, awareness, culture, self-efficacy, framework, governance, AMC
ProQuest Dissertations and Theses	HIPAA, security, compliance, AMC
Science Direct	HIPAA, security, compliance, AMC

In this review, the author presented the literature on the constructs of management support, security awareness, security culture, and computer self-efficacy, security effectiveness, and security behavior in the context of the larger construct of information

security knowledge. First, the literature on the HIPAA Security Rule was reviewed, followed by the literature on security behavior and then security effectiveness, both of which were dependent variables in this study. Subsequently, the literature on management support, security awareness, security culture, and computer self-efficacy, the independent variables in the study, was reviewed.

HIPAA Security Rule

> The U.S. Congress enacted HIPAA on August 21, 1996 to improve portability and continuity of health insurance coverage in the group and individual markets, to combat waste, fraud, and abuse in health insurance and health care delivery, to promote the use of medical savings accounts, to improve access to long-term care services and coverage, to simplify the administration of health insurance, and for other purposes. (HIPAA of 1996 Pub. L. No. 104-191, 110 Stat. 1936, 1996, p. 1)

Helms et al. (2008) stated, "HIPAA is the most significant Federal legislation affecting the U.S. health care industry since the Medicare and Medicaid legislation of 1965" (p. 84). The administrative simplification provisions of Title II of HIPAA were established to create a comprehensive set of rules regulating, among other things, the security of medical information (Bianchi, 2009). The HIPAA Security Rule became effective on April 21, 2003, with compliance mandated by April 21, 2005 (Happ, 2006; Schulman, 2006).

The HIPAA Security Rule established a new security framework for the health care industry (Drumke, 2008). As a result, the U.S. Congress stipulated four general

requirements for covered entities: (a) ensure the confidentiality, integrity, and availability of ePHI; (b) safeguard against reasonably anticipated data security threats; (c) protect against reasonably anticipated impermissible uses and disclosures of ePHI; and (d) ensure compliance with the HIPAA Security Rule (HIPAA, 2005e). Drumke noted that the U.S. Congress delegated the full responsibility for developing and enforcing the HIPAA Security Rule requirements to HHS.

HHS exercised its responsibility and promulgated the security standards (45 CFR parts 160, 162, and 164) within the administrative simplification provision under Subtitle F of Title II (Happ, 2006). The HIPAA Security Rule (45 CFR Parts 160 and 164) specified a series of administrative, technical, and physical security safeguards for health plans, health clearinghouses, and certain health care providers to ensure ePHI confidentiality (Bianchi, 2009). As noted by Helms et al. (2008), the three security safeguards were classified as either required or addressable. Required safeguards must be adopted and implemented, while addressable safeguards can be more flexible and implemented by the covered entities as needed (Helms et al.). The administrative safeguards include controls for security management, workforce security, information access management, security awareness and training, security incident procedures, disaster recovery, evaluation, and business associate contracts (Bianchi; Schulman, 2006). The physical safeguards include specifications for facility access controls, workstation use, workstation security, and device and media controls (Bianchi; Schulman). The technical safeguards include standards for access control, audit controls, integrity, person or entity authentication, and transmission security (Bianchi; Schulman).

The HIPAA Security Rule was designed to be scalable and flexible as well as to allow covered entities "to choose the specific means by which to reasonably and appropriately implement the Rule's requirements" (Hoffman & Podgurski, 2007, p. 7). Medlin and Cazier (2007) stated that health care organizations should take reasonable and appropriate steps to limit the disclosure of an individual's personal health information and secure access to electronic patient records.

To enforce the requirements of the HIPAA Security Rule, the secretary of HHS was authorized by the U.S. Congress to impose civil monetary penalties on any person failing to comply with HIPAA security standards (Social Security Act, 2005b). The maximum civil fine was $100 per violation and up to $25,000 for all violations of an identical requirement during a calendar year (HIPAA, 2005c). Criminal penalties were up to $50,000 or one year in prison for violations in which a person uses a unique health identifier, obtains a unique health identifier relating to an individual, or discloses a unique health identifier to another person (Social Security Act, 2005b). A person committing the violation under false pretense could be fined up to $100,000, receive a prison sentence of up to five years, or both (Social Security Act, 2005b). Finally, a person could be fined up to $250,000, sentenced up to ten years in prison, or both if the violation is committed with "the intent to sell, transfer, or use a unique health identifier for commercial gain, malicious harm, or personal gain" (Social Security Act, 2005a p. 12).

Data Security Breaches

At present, information security and privacy are major concerns in the health care domain (Huang et al., 2008). According to the 2009 HIMSS Security Survey, one-third of the 196 respondents reported that their organization had at least one known case of

medical identity theft, with only one-half having a plan in place for responding to security breach threats or incidents (Gallagher, 2009). Respondents characterized their own maturity level as mid-range, with an average score of 4.27 on a scale of 1 to 7. Approximately 60% of the respondents reported that their organization spent 3% or less of their IT budget on information security, indicating that few additional resources have been applied to information security since the 2008 HIMSS Security Survey. Fewer than one-half of the respondents indicated that their organization had either a formally designated chief information security officer or chief security officer.

The 2009 HIMSS Security Survey results also indicated that 25% of the surveyed organizations have not conducted a formal risk analysis (Gallagher, 2009). Of those organizations that actively conduct formal risk analyses, 52% indicated that "patient data at their organization was found to be at risk as a result of both a lack of effective security controls and a lack of adequate policies and/or procedures" (p. 3). Another 15% of the respondents indicated that their organization's patient data was at risk as a result of a lack of effective security controls in place at their organization, while 5% reported "that their organization's patient data was at risk because their organization did not have adequate policies and procedures in place" (p. 4). Moreover, 33% of the responding organizations noted that they did not use available technologies to secure data in transmission, such as encryption, while fewer than one-half of the responding organizations reported encrypting stored data.

According to the 2009 Security Mega Trends Survey of 577 information security practitioners, stopping cyber crime and data breaches was reported to be a top security concern (Ponemon, 2008). The 2009 Ernst & Young Business Risk Report identified

regulation and compliance as the only critical risk in the Life Sciences area (Ernst & Young, 2009). Based on the 2009 Computer Security Institute (CSI) Computer Crime and Security Survey of 443 information security and information technology professionals in the U.S., Peters (2009) reported that theft of PHI through all causes other than mobile device theft was the second most expensive security incident, with losses reported at $710,000. Despite the fact that only 7.7% of respondents categorized their organizations as being in the health services industry, 57.1% of the respondents stated that their organization had to comply with HIPAA. According to Peters, "more respondents said that HIPAA applied to their organization than any other law or industry regulation" (p. 3). Moreover, the AAMC identified HIPAA security compliance as a high priority objective (AAMC, 2009d).

The 2008 $(ISC)^2$ Global Information Security Workforce Study reported that "the majority of respondents rated preventing damage to an organization's reputation as their highest priority" (Frost & Sullivan, 2008, p. 5). According to Moynihan (2007), organizations that publically disclose data security breaches such as database intrusion and laptop theft risk the possibility of reduced customer confidence. For example, Hasemyer (2009) reported that the recent unauthorized access by hackers to the University of California at San Diego Medical School computer systems acts as a "reminder that hospitals and other medical facilities must remain vigilant" (para. 9). Therefore, in addition to complying with HIPAA regulatory requirements, health care organizations must prioritize data security breach prevention to reduce damage to their reputation (Fritsche & Rodgers, 2007).

Growth of Health Care IT Infrastructure

According to Thielst (2007), the rapid adoption of health information technology was supported by President George W. Bush, who set a goal in 2004 to create an electronic medical record for every American by 2014. As a result of the continued growth of health information technology and an increasing dependency on electronic medical records, Li and Shaw (2008) indicated that a wide range of security concerns must be addressed. As a consequence, health care leaders are under continued pressure to ensure compliance with the HIPAA Security Rule (Li & Shaw; Thielst).

The increased adoption of networked computers, along with the growing reliance on computer security to protect IT assets and provide a competitive business advantage, has necessitated increased security requirements (Hale & Brusil, 2007; Kruck & Teer, 2008; Pirim, James, Boswell, Reithel, & Barkhi, 2008). However, "more than a decade after the passage of HIPAA, concerns about the privacy and security of personal health information remain a major policy issue" (Greenberg & Ridgely, 2009, p. 450).

According to Bhatti, Moidu, and Ghafoor (2006), this is due in part to the emergence of new technology developments and regional health information organizations. Bhatti et al. argued that the pervasive and ubiquitous access to health care information from outside of traditional hospital boundaries has put increasing demands on the underlying security mechanisms. This widespread accessibility of user data has become a liability to health care organizations and their patients, creating easier access to sensitive materials and inviting crimes of opportunity ("Responsible information management," 2009). Further, as indicated by Greenberg and Ridgely, the implementation of the Nationwide

Health Information Network has created new security implications, none of which was considered when the HIPAA Security Rule was developed.

Enforcement of the HIPAA Security Rule

The federal government recently initiated a comprehensive HIPAA Security Rule audit of covered entities, with stringent financial penalties issued for noncompliance (Hourihan, 2009). HHS engaged the Office of Inspector General to perform its first HIPAA security compliance review when it audited Piedmont Hospital of Atlanta in 2007 (Ruzic, 2009). According to Ruzic, the Office of Inspector General found significant vulnerabilities, including unprotected ePHI. As a result, "the audit caught the attention of many covered entities who had long ago assumed that since no HIPAA enforcement actions had occurred since 2003, that there would never be any such actions" (Herold, 2009b, para. 5).

In addition to the HHS audit, CMS contracted Price Waterhouse Coopers to conduct 26 more HIPAA Security Rule compliance audits during 2008 and 2009 (Holland, 2009). In 2009, HHS transferred the authority for the administration and enforcement of the HIPAA Security Rule from CMS to the Office for Civil Rights (Conn, 2009). Conn reported that, because the Office of Civil Rights is also responsible for the enforcement of the HIPAA Privacy Rule, combining HIPAA Privacy Rule and HIPAA Security enforcement will eliminate duplication, increase efficiency, and lead to stricter enforcement of both federal rules. As a consequence of these federal audits, several health care organizations subsequently received fines up to $2.25 million for HIPAA compliance violations. (Bakhtiari, 2009; "HIPAA violation costs CVS," 2009).

Extension of the HIPAA Security Rule

New federal regulations and state laws have significantly increased the requirements of the HIPAA Security Rule and the consequences for noncompliance (Bianchi, 2009; Rath, 2009; Swearingen, 2009). The passage of the Health Information Technology for Economic and Clinical Health (HITECH) Act on February 17, 2009, as part of the American Recovery and Reinvestment Act (ARRA) of 2009, has substantially altered and extended the HIPAA Security Rule compliance requirements (Aguilar, 2009: Davis, 2009). As a result of the HITECH Act, penalties for HIPAA Security Rule noncompliance were significantly increased (Maffeo, 2009).

According to Barlas (2009), more stringent requirements were enacted for breach notifications of unsecured PHI. State attorneys were authorized to bring civil action in federal district court against HIPAA Security Rule violators (Bakhtiari, 2009). Business associates are now held accountable for full HIPAA Security Rule compliance (Blades, 2009). Brown (2009b) noted that monetary fines for noncompliance were substantially increased, and new guidance for stricter encryption and destruction methods has been established (Dowell, 2009). Frequent HHS audits of HIPAA-covered entities and formal investigations of HIPAA-related complaints were mandated (Davis, 2009). Holloway (2009) stated that the new rules will have varying effective dates through 2012, which will make implementation and communication of the rules more challenging for organizations subject to the HIPAA Security Rule. Consequently, there is a need to investigate HIPAA security compliance in health care organizations, specifically in AMCs that represent the leading U.S. medical schools, teaching hospitals and health systems, and academic societies (Steinbrook, 2009).

Security Behavior

More attention needs to be given to the social and behavioral aspects of information security among AMCs (Guzman et al., 2008; Hazari, 2005; Huebner & Britt, 2006; Pattinson & Anderson, 2007). According to Ma et al. (2008), because information security is more of a human problem than a pure technical problem, practitioners should pay more attention to the cultural aspects of information security. The author identified numerous user acceptance models in the literature, including the Technology Acceptance Model (TAM) and TAM2 (Davis, 1989; Venkatesh & Davis, 2000). However, further research on the generalizability of factors associated with technology acceptance (TA) and user behavioral studies is needed (Ball & Levy, 2008), particularly in the domain of information security (Dinev & Hu, 2007; Hazari et al., 2008; Novakovic et al., 2009). Many information security breaches in the workplace have been attributed to the failure of employees to comply with organizational security policies (Chan et al., 2005). As a result, Chan et al. stated that "attention needs to be paid to learning why non-compliant behavior takes place so that appropriate measures for curbing the occurrence of such behavior can be found" (p. 18). Because employees are responsible for numerous security breaches, Logan and Noles (2008) recommended the assessment of operations and services enabled by internal security controls.

Technology Acceptance Literature

Dinev and Hu (2007) stated that an understanding of security behavior requires an examination of the technology acceptance literature. This examination includes a review of the theory of reasoned action (TRA; Ajzen & Fishbein, 1980; Fishbein & Ajzen, 1975), the theory of planned behavior (TPB; Ajzen, 1985, 1991), TAM (Davis, 1989;

Davis, Bagozzi, & Warshaw, 1989), TAM2 (Venkatesh & Davis, 2000; Venkatesh, Morris, Davis, & David, 2003), and the unified theory of acceptance and use of technology (UTAUT) model (Venkatesh et al.).

Because TRA posits that the most significant predictor of behavior is intention, it is useful in describing behavior (Fishbein & Ajzen, 1975). TRA asserts that factors that influence behavior do not do so directly but rather indirectly by influencing other factors (Davis et al., 1989). According to Cazier, Wilson, and Medlin (2007), TRA represents a rational decision-making approach to the prediction of behaviors in which individual beliefs are mediated by attitude and behavioral intentions. However, although TRA has strong behavioral elements and predicts intention well, it is limited in explanatory power and does not address other factors that may influence technology acceptance (Sun & Zhang, 2006; Venkatesh & Davis, 1996).

Ajzen (1985, 1988, 1991) developed TPB as an extension of TRA. TPB posits that a user's behavior is determined by his or her intention to perform the behavior. Ajzen identified attitude toward the behavior, subjective norm, and perceived behavioral control as the three factors affecting behavioral intention. The majority of TPB models argue that attitude has a direct relationship between beliefs and intention (Dinev & Hu, 2007). Although some TPB models have validated other factors moderating attitude (Pavlou & Fygenson, 2006; Taylor & Todd, 1995), TPB models have shown only a modest degree of predictive power for behavior intentions (Dillon & Morris, 1996).

In response to the limitations of TRA and TPB in predicting and explaining user acceptance of a new technology, Davis (1989) and Davis et al. (1989) developed TAM. As indicated by Ball and Levy (2008), TAM is the classical IS model developed to

explain computer-usage behavior and constructs associated with acceptance of technology. TAM considers two determinants, ease of use and perceived ease of use, and their relationship to behavioral intention to use and actual system usage (Davis; Davis et al.). Similar to TRA and TPB, TAM has become popular among researchers due to its parsimonious approach and extensive empirical support in the literature (Lallmahamood, 2007). TPB and TAM have been shown to be "robust in explaining and predicting user behavior toward technological innovations in general, as evident in the sheer number of studies based on these two frameworks" (Dinev & Hu, 2007, p. 390).

According to Novakovic et al. (2009), UTAUT was developed through a review and consolidation of eight prior technology acceptance models to explain IS usage behavior. These technology acceptance models included TRA (Fishbein & Ajzen, 1975), TAM (Davis, 1989), motivational model (Vallerand, 1997), TPB (Ajzen, 1991), combined theory of planned behavior/technology acceptance model (Taylor & Todd, 1995), model of PC utilization (Thompson, Higgins, & Howell, 1994), innovation diffusion theory (Rogers, 1962), and social cognitive theory (Bandura, 1986). In a longitudinal study, Venkatesh et al. (2003) observed that UTAUT contains a broad range of influences and accounts for 70% of the variance in IS behavior usage.

Security Behavior Literature

Security behavior has been examined in the information security literature (Da Veiga & Eloff, 2007; Kruck & Teer, 2008; Rotvold, 2008; Tsohou et al., 2008). Researchers have investigated security behavior in terms of IS misuse (D'Arcy & Hovav, 2009), technology awareness (Dinev & Hu, 2007), password usage (Teer, Kruck, & Kruck, 2007), and leadership (Neufeld, Dong, & Higgins, 2007). Security behavior has been

determined to be a key factor affecting health care organizations' security effectiveness and HIPAA security compliance (Chan et al., 2005; Johnston & Warkentin, 2008; Novakovic et al., 2009).

Based on a study of 104 employees from two IT intensive organizations in the logistics and petrochemical industries, Chan et al. (2005) found that breaches in security generally result from noncompliant employee behavior. Chan et al. adapted the dependent variable, compliant behavior, from Griffin and Neal's (2000) definition of safety compliant behavior. Chan et al. defined compliant information security behavior as "the set of core information security activities that need to be carried out by individuals to maintain information security as defined by information security policies" (p. 22). Chan et al. determined that perception of information security climate and self-efficacy positively affect employees' compliant behavior. The employee compliant behavior model is shown in Figure 2.

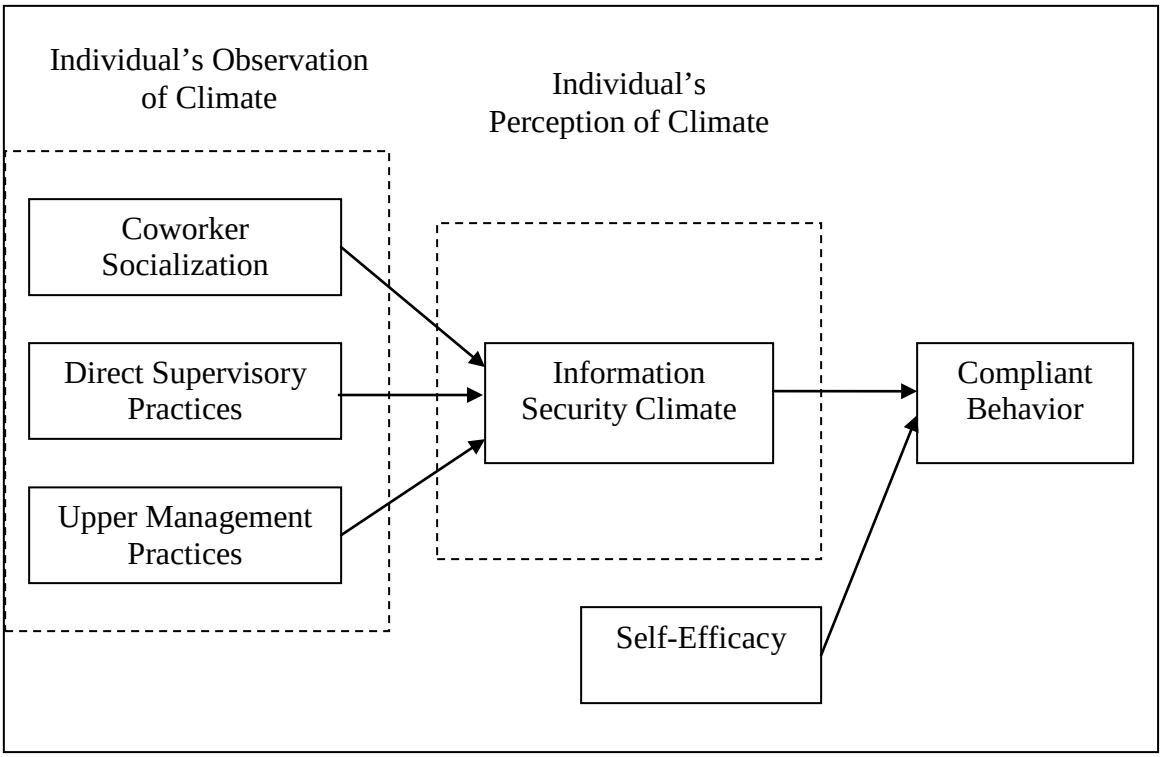

Figure 2. The employee compliant behavior model showing the effect of information security climate and self-efficacy on compliant behavior (Chan et al., 2005, p. 23).

Johnston and Warkentin (2008) developed a conceptual framework that includes TPB, TAM, UTAUT, models of self-efficacy, and the construct of perceived organizational support. Johnston and Warkentin did not include a direct measure of actual HIPAA compliance behavior. Nonetheless, they found that perceived organizational support and self-efficacy exerted a positive influence on HIPAA compliance behavioral intent. The HIPAA compliance model is shown in Figure 3.

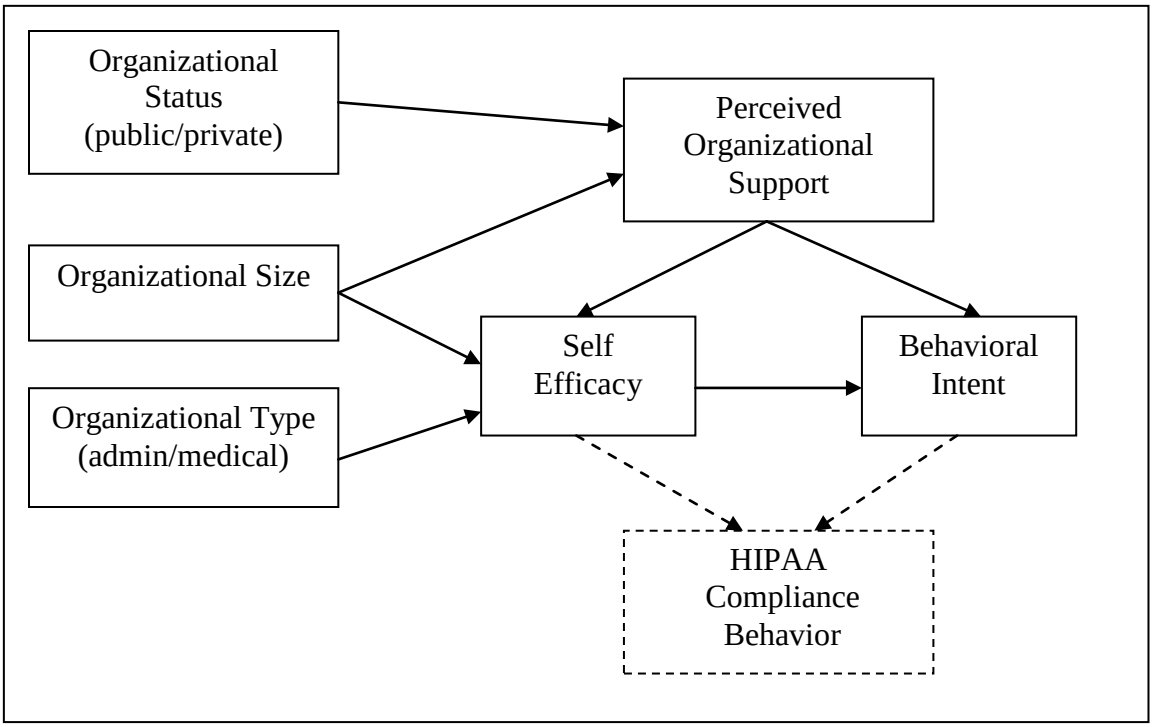

Figure 3. The HIPAA compliance model showing the relationship of self-efficacy and behavioral intent to HIPAA compliance behavior (Johnston & Warkentin, 2008, p. 7).

In a study of 111 computer users in Australia, Novakovic et al. (2009) derived a model from UTAUT for examining the effect of ease of use and secure behavior intention on secure usage. Novakovic et al. defines secure behavior intention as an individual's intention to use technology in a secure fashion, while secure usage refers to a user's actual usage of technology in a secure manner. These researchers found that technology that was difficult to use caused a decrease in secure user behavior and user security compliance. Further, Novakovic et al. concluded that an individual's intention to behave securely is a good indicator of his or her actual behavior. Novakovic et al.'s model depicting the influence of secure behavior intention on secure usage is shown in Figure 4.

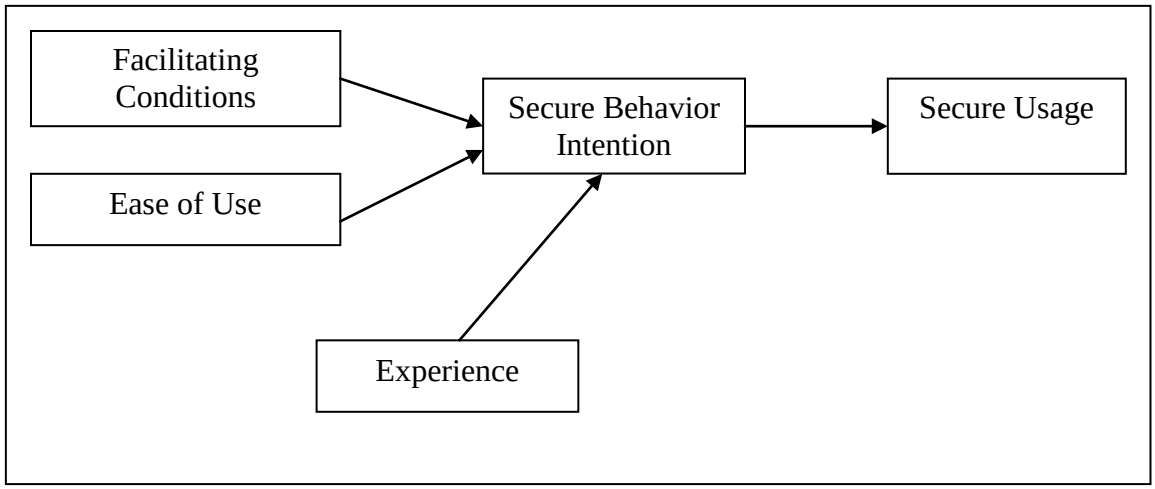

Figure 4. Model showing the influence of secure behavior intention on secure usage (Novakovic et al., 2009, p. 24).

A summary of the security behavior literature is presented in Table 2.

Table 2. Summary of the Security Behavior Literature

Study	Methodology	Sample	Instrument /Factor	Main Findings or Contribution
Ajzen (1985)	Theoretical	Classical study	TPB, Attitude, Subjective Norm, Perceived Behavioral Control, and Behavioral Intention	Developed TPB as an extension of TRA. A user's behavior is determined by his or her intention to perform the behavior. Attitude toward the behavior, subjective norm, and perceived behavioral control were found to affect behavioral intention.
Ajzen (1988)	Theoretical	Classical study	TPB, Attitude, Subjective Norm, and Perceived Behavioral Control, Behavioral Intention	Developed TPB as an extension of TRA. A user's behavior was determined by his or her intention to perform the behavior. Attitude toward the behavior, subjective norm, and perceived behavioral control were found to affect behavioral intention.
Ajzen (1991)	Theoretical	Classical study	TPB, Attitude, Subjective Norm, and Perceived Behavioral Control, Behavioral Intention	Developed TPB as an extension of TRA. A user's behavior was determined by his or her intention to perform the behavior. Attitude toward the behavior, subjective norm, and perceived behavioral control were found to affect behavioral intention.

Table continues.

Table 2 (Continued)

Study	Methodology	Sample	Instrument /Factor	Main Findings or Contribution
Ajzen and Fishbein (1980)	Theoretical	Classical study	TRA	Developed the theory of reasoned action.
Ball and Levy (2008)	Survey	111 instructors teaching IS and non-IS courses at a small private university in the southeastern U.S.	CSE, computer abuse, and experience with the use of technology on intention to use	Only CSE influences intention to use and behavior.
Bandura (1986)	Theoretical	Classical study	CSE and SB	Developed social cognitive theory to address technology acceptance.
Cazier, Wilson, and Medlin (2007)	Survey	331 undergraduate business students at a major U.S. university.	TRA, perceived ease of use, perceived use, behavior intention, perceived privacy risk likelihood, and perceived privacy risk harm	TRA represents a rational decision-making approach to the prediction of behaviors in which individual beliefs were mediated by attitude and behavioral intentions.

Table continues.

Table 2 (Continued)

Study	Methodology	Sample	Instrument /Factor	Main Findings or Contribution
Chan, Woon, and Kankanhalli (2005)	Survey	104 employees from two IT intensive organizations in the logistics and petrochemical industries	Information security climate, self-efficacy, MS, and compliant behavior	Coworker socialization, direct supervisory practices, and upper management practices affected information security climate. Information security climate and self-efficacy influenced compliant behavior.
D'Arcy and Hovav (2009)	Survey	238 employed working professionals taking MBA classes at two mid-Atlantic U.S. universities	CSE, SA, IS misuse behavioral intention	CSE affected SA effectiveness and IS misuse behavioral intention in terms of unauthorized access and unauthorized modification.
Da Veiga and Eloff (2007)	Theoretical	Commentary	MS, SA, SC, SB, and SE	MS and SA were needed for an acceptable level of information security culture and behavior.
Davis (1989)	Theoretical and survey	152 users were tested on four application programs in two studies	TAM constructs including perceived ease of use and perceived use	Developed TAM to address limitations of TRA and TPB by examining ease of use and perceived ease of use, and their relationship to behavioral intention to use and actual usage.

Table continues.

Table 2 (Continued)

Study	Methodology	Sample	Instrument /Factor	Main Findings or Contribution
Davis, Bagozzi, and Warshaw (1989)	Theoretical and survey	107 full time MBA students	TAM constructs, including attitude towards behavior, subjective norm, perceived use, perceived ease of use, and behavior intention	Factors influencing behavior did so indirectly by influencing other factors. Perceived use and perceived ease of use was a significant determinant of behavior intention.
Dillon and Morris (1996)	Literature Review	Commentary	TPB, Behavior Intention	Determined TPB models exerted only a modest degree of predictive power for behavior intentions.
Dinev and Hu (2007)	Theoretical and survey	332 IS professionals and students of a large Southeastern university in the U.S.	SA, attitudes toward behavior, subjective norm, behavioral intention, perceived behavior control, controllability, self-efficacy, perceived ease of use, and perceived usefulness	In the context of use of technology awareness and protective technologies, SA was found to influence attitudes toward behavior, subjective norm, behavioral intention, and perceived behavior control. SA influenced controllability, self-efficacy, perceived ease of use, and perceived use.
Fishbein and Ajzen (1975)	Theoretical and survey	N/A	TRA constructs, including attitude toward behavior and subjective norm	Developed TRA. The most significant predictor of behavior was intention. Thus it was useful in describing behavior.

Table continues.

Table 2 (Continued)

Study	Methodology	Sample	Instrument /Factor	Main Findings or Contribution
Griffin and Neal (2000)	Theoretical	Commentary	Safety compliant behavior	SB was correlated to information security compliance.
Guzman, Stam, and Stanton (2008)	Semi-structured interviews	32 IT personnel and 89 other employees from eight non-profit organizations, including a university and hospital	SC and SB	Organizational and occupational culture positively influence HIPAA security compliant behavior in AMCs.
Hazari, Hargrave, and Clenney (2008)	Survey	179 undergraduate and graduate business school students in a state university in the southeastern U.S.	Attitudes, subject norm, and perceived behavioral control, (CSE) on SA, SE, and SB	Social cognition factors, such as attitude, subject norm, and perceived behavioral control influenced SA and information security behavior effectiveness.
Huebner and Britt (2006)	Theoretical	Commentary	SC and SB	The cultural aspects of an enterprise were vital to the success of a security program. Behavioral aspects of security, such as emotional intelligence, structural theory, and social network analysis, influence enterprise security.

Table continues.

Table 2 (Continued)

Study	Methodology	Sample	Instrument /Factor	Main Findings or Contribution
Johnston and Warkentin (2008)	Survey	208 health care professionals from various health care facilities located in Texas, Alaska, Louisiana, Mississippi, Virginia, Alabama, Arizona, Michigan, Pennsylvania, and Florida	Organizational status, organizational size, organizational type, perceived organizational support, self-efficacy, behavioral intent, and HIPAA compliant behavior	Perceived organizational support, and self-efficacy exerted a positive influence on HIPAA compliance behavioral intent. Security awareness affected HIPAA compliant behavior.
Kruck and Teer (2008)	Survey	355 undergraduate students at one large state university on the east coast.	SA on SB	SA influenced individuals' security practices.
Lallmahamood (2007)	Survey	197 executives, managers, executive MBA students, and college students from the Malaysian Institute of Management	Perceived security, perceived ease of use, perceived use, and intention to use	Perceived security influenced perceived ease of use, perceived use, and intention to use.

Table continues.

Table 2 (Continued)

Study	Methodology	Sample	Instrument /Factor	Main Findings or Contribution
Logan and Noles (2008)	Case study	A regional, 893-bed hospital with more than 5,000 employees in the mid-Atlantic region of the U.S.	MS, SA, and SB	MS and SA influenced HIPAA security compliant behavior.
Ma, Johnston, and Pearson (2008)	Survey	354 certified information security professionals from the International Information Systems Security Certificate Consortium	MS, SA, SC, SE, and SB.	MS influenced SA and HIPAA compliant information security behavior. SC, and organizational self-efficacy were positively correlated to effective information security management.
Neufeld, Dong, and Higgins (2007)	Survey	209 employees from seven mid-size-to-large Canadian manufacturing companies	MS and SB	MS influenced SB in the context of IT adoption and use behavior.

Table continues.

Table 2 (Continued)

Study	Methodology	Sample	Instrument /Factor	Main Findings or Contribution
Novakovic, McGill, and Dixon (2009)	Survey	111 computer users in Australia	Perceived usefulness of security, ease of use, facilitating conditions, secure behavior intention, and secure usage based on UTAUT.	Facilitating conditions, ease of use and experience influenced secure behavior intention. Secure behavior intention influenced secure usage in terms of effective password usage.
Pattinson and Anderson (2007)	Survey	Two pilot studies consisting of groups of 35 and 40 undergraduate students at the University of South Australia	SA, SE, and SB	User education and training, and understanding user behavior towards risk culture were needed to achieve an acceptable level of information security.
Pavlou and Fygenson (2006)	Theoretical, longitudinal study, and survey	312 online consumers	TPB, Attitude toward behavior	Additional factors moderated attitude toward behavior.
Rogers (1962)	Theoretical	Commentary	TAM	Developed innovation diffusion theory to address technology acceptance.

Table continues.

Table 2 (Continued)

Study	Methodology	Sample	Instrument /Factor	Main Findings or Contribution
Rotvold (2008)	Survey	144 business professionals, managers, IT administrators, and educators from various organizations, including health care	MS, SA, SC, and SE	MS influenced SA, and that SA influenced SC and information security program effectiveness.
Sun and Zhang (2006)	Theoretical and literature review	Commentary	Subjective norm, perceived ease of use, perceived use	TRA was limited in its explanatory power and does not address other factors that may influence technology acceptance.
Taylor and Todd (1995)	Theoretical and survey	786 student users of a computing resource center	TPB, attitude toward behavior, subjective norm, perceived behavioral control, behavioral intention, perceived usefulness, compatibility, ease of use, and usage	Developed a combined TPB/TAM called DTPB. Validated that additional factors moderate attitude toward behavior.
Teer, Kruck, and Kruck (2007)	Survey	86 undergraduate students from one large four-year public state university	SA and SB	SA influenced SB in terms of password usage.

Table continues.

Table 2 (Continued)

Study	Methodology	Sample	Instrument /Factor	Main Findings or Contribution
Thompson, Higgins, and Howell (1994)	Theoretical	Classical study	TAM	Developed a model of PC utilization to address technology acceptance.
Tsohou, Kokolakis, Karyda, and Kiountouzis (2008)	Theoretical	MS, SA, SE, and SB	MS, SA, SE, and SB	MS affected SA, and SA influenced SE in the context of AMCs. SA influenced good end-user security behavior.
Vallerand (1997)	Theoretical	Commentary	TAM and behavior	Developed the hierarchical model of intrinsic and extrinsic motivational to explain technology acceptance.
Venkatesh and Davis (1996)	Theoretical and Survey	Three experiments involving 40 MBA students at Boston University, 36 undergraduate students at Temple University, and 32 part-time MBA students at the University of Minnesota	CSE, behavior, and perceived ease of use	TRA was limited in its explanatory power and did not address other factors that may influence technology acceptance.

Table continues.

Table 2 (Continued)

Study	Methodology	Sample	Instrument /Factor	Main Findings or Contribution
Venkatesh and Davis (2000)	Theoretical and four longitudinal field studies	156 employees in four organizations	TAM2 constructs, including subjective norm, image, job relevance, experience, perceived use, perceived ease of use, intention to use, and usage behavior	Extended TAM to develop TAM2. Demonstrated that social influence and cognitive instrumental processes affected user acceptance.
Venkatesh, Morris, Davis, and David (2003)	Theoretical and survey	215 users surveyed for primary data and 133 users surveyed for cross-validation from two organizations.	Performance expectancy, effort expectancy, social influence, facilitating conditions, gender, age, experience, voluntariness of use describing TAM2 and UTAUT	UTAUT broadly influenced and affected IS behavior usage. UTAUT outperformed the eight individual models in predicting technology acceptance.

Security Effectiveness

A better understanding of information security effectiveness among AMCs is needed (Chang & Lin, 2007; Knapp et al., 2006; Tsohou et al., 2008). D'Arcy and Hovav (2009) indicated that understanding the factors affecting the effectiveness of security countermeasures has been a consistent theme in the literature. Due to the disappointing state of information security in organizations, Dhillon and Backhouse (2001) called for

more empirical research to develop key information security principles (Knapp et al., 2007). According to Chang and Yeh (2006), information security effectiveness has been seriously questioned due to the continued high volume of security-related incidents and subsequent financial losses. Moreover, Pumphrey, Trimmer, and Beachboard (2007) found that health care management needs to give more attention to developing effective security policies to address HIPAA Security Rule compliance.

Security Effectiveness Literature

Security effectiveness has been frequently reviewed in the IS security literature (Chang & Yeh, 2006; Filipek, 2007; Knapp et al., 2006; Knapp et al., 2007; Lineberry, 2007; Novakovic et al., 2009; Smith & Jamieson, 2006; Tsohou et al., 2008). Scholars have investigated security effectiveness in terms of acceptable security (Chang & Ho, 2006; Pattinson & Anderson, 2007), effective computer security (Knapp & Boulton, 2006), security management effectiveness (Chang & Lin, 2007; Drew, 2007; Moreira, Martimiano, Brandão, & Bernardes, 2008; Tang, 2008; Winkel, 2007; "Worries over corporate reputation," 2008), effective security strategy (Moynihan, 2007), effective security programs (Jahankhani et al., 2007), effective security measures and countermeasures (D'Arcy & Hovav, 2009; Rennie & Shore, 2007), effective security behavior (Hazari et al., 2008), effective security awareness (D'Arcy & Hovav), effective security culture (Da Veiga & Eloff, 2007), and security professional effectiveness (Hawkey, Muldner, & Beznosov, 2008). Security effectiveness is a key construct affecting security behavior and HIPAA security compliance in health care (Chang & Lin; D'Arcy & Hovav; Hazari et al.).

The effectiveness of security countermeasures in reducing the risk of computer abuse was first hypothesized in the conceptual studies of Martin (1973), Klete (1975), and Madnick (1978). Straub (1990) referred to IS security effectiveness as the ability of IS security measures to protect against "the unauthorized and deliberate misuse of assets of the local organizational information system by individuals, including violations against hardware, programs, data, and computer service" (p. 4). Based on a survey of 1,211 randomly selected organizations, Straub used the criminological theory of general deterrence to investigate whether a management decision to invest in IS security would result in more effective control of computer abuse. Ehrlich (1973) and Blumstein, Cohen, and Nagin (1978) noted that general deterrence theory predicts that potential offenders will be inhibited from committing anti-social acts when the risk of punishment is high and penalties for violation are severe. Straub found that security countermeasures that include deterrent administrative procedures and preventive security software result in lower computer abuse, thus demonstrating that IS security is effective.

Kankanhalli, Teo, Tan, and Wei (2003) further advanced the theory of IS security effectiveness by developing and testing an integrative model of IS security effectiveness. Through an empirical study of IS managers from small-, medium-, and large-sized enterprises, Kankanhalli et al. observed that top management support, greater deterrent efforts, and preventative measures lead to enhanced IS effectiveness. Kankanhalli et al.'s model of IS security effectiveness is shown in Figure 5.

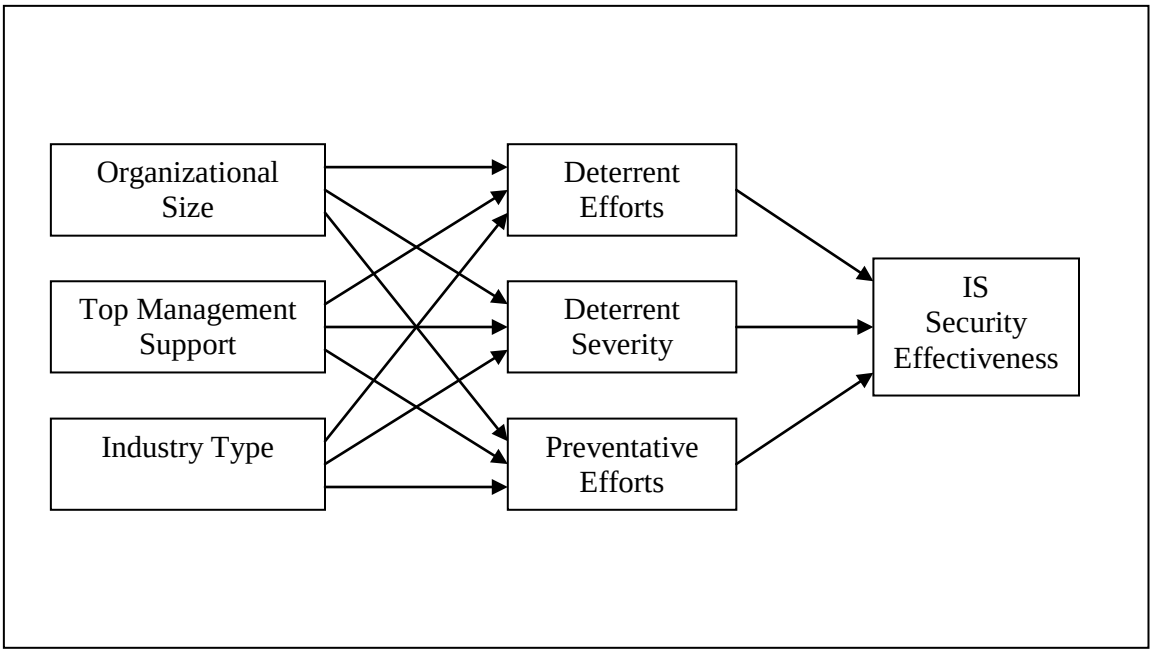

Figure 5. The original model of IS security effectiveness (Kankanhalli et al., 2003, p. 143).

Chang and Lin (2007) studied 108 senior IT managers and professionals from various industries, including health care. They found that organizational culture and management support had a positive influence on security effectiveness. The authors observed that a security framework, specifically ISO/IEC 17799, is needed to help organizations attain "an acceptable level of information resource protection" (p. 440). Further, Chang and Lin determined that effectiveness was significantly correlated to confidentiality, integrity, and availability. According to HIPAA (2005e), the HIPAA Security Rule specifies that each covered entity must ensure the confidentiality, integrity, and availability of ePHI that it creates, receives, maintains, or transmits. Confidentiality means that data and/or information are not disclosed to unauthorized persons or processes, integrity means that data and/or information are not altered or destroyed in an unauthorized manner, and

availability means that data and/or information are accessible and useable upon demand by an authorized person (HIPAA, 2005d).

A summary of the security effectiveness literature is presented in Table 3.

Table 3. Summary of the Security Effectiveness Literature

Study	Methodology	Sample	Instrument /Factor	Main Findings or Contribution
Blumstein, Cohen, and Nagin (1978)	Theoretical	Classical study	General deterrence theory	Potential offenders were inhibited from committing anti-social acts when the risk of punishment was high and penalties for violation were severe.
Chang and Ho (2006)	Survey	59 senior managers from various organizations, including health care	MS and SE	MS influenced SE.
Chang and Lin (2007)	Survey	108 senior IT managers and professionals from various industries, including health care	SC and MS on SE	Organizational culture and MS positively influenced information security management effectiveness.
Chang and Yeh (2006)	Survey	109 managers of large Taiwan firms	SA, MS, and SE	SA and MS were required to reduce information security threats and achieve effective information security.

Table continues.

Table 3 (Continued)

Study	Methodology	Sample	Instrument /Factor	Main Findings or Contribution
D'Arcy and Hovav (2009	Survey	238 employed working professionals taking MBA classes at two mid-Atlantic U.S. universities	CSE, SA, IS misuse behavioral intention	CSE affected SA effectiveness and IS misuse behavioral intention in terms of unauthorized access and unauthorized modification.
Da Veiga and Eloff (2007)	Theoretical	Commentary	MS, SA, SC, SB, and SE	MS and SA were needed for an acceptable level of information security culture and behavior.
Dhillon and Backhouse (2001)	Theoretical	Commentary	SA and SE	Identified the need for increased SA, education, and training in order to achieve effective security.
Drew (2007)	Theoretical	Commentary	MS, SC, and SE	MS and organizational culture positively correlated to perceived risk and an effective risk management program.
Ehrlich (1973)	Theoretical	Classical study	General deterrence theory	Potential offenders were inhibited from committing anti-social acts when the risk of punishment was high and penalties for violation were severe.

Table 3 (Continued)

Study	Methodology	Sample	Instrument /Factor	Main Findings or Contribution
Table continues.				
Filipek (2007)	Survey	Multiple organizations from Europe	SA and SE	Training was the most effective technique to change staff behavior and increase information security awareness.
Hawkey, Muldner, and Beznosov (2008)	Case study	36 IT professionals from large academic organization	SC and SE	Organizational culture influenced IT security professional effectiveness.
Hazari, Hargrave, and Clenney (2008)	Survey	179 undergraduate and graduate business school students in a state university in the southeastern U.S.	Attitudes, subject norm, and perceived behavioral control, (CSE) on SA, SE, and SB	Social cognition factors, such as attitude, subject norm, and perceived behavioral control influenced SA and information security behavior effectiveness.
Jahankhani, Fernando, Nkhoma, and Mouratidis (2007)	Theoretical	Commentary	MS and SE	MS influenced SE.
Kankanhalli, Teo, Tan, and Wei (2003)	Survey	63 IS managers from multiple professional organizations	MS and SE	Top management support, greater deterrent efforts, and preventative measures led to enhanced IS security effectiveness.

Table 3 (Continued)

Study	Methodology	Sample	Instrument /Factor	Main Findings or Contribution
Table continues.				
Klete (1975)	Theoretical	Commentary	SE	The effectiveness of security countermeasures correlated to the risk of computer abuse occurrence.
Knapp and Boulton (2006)	Theoretical	Commentary	MS, SC, SA, and SE	MS, SC, and SA influenced SE.
Knapp, Marshall, Rainer, and Ford (2006)	Survey	220 certified information systems security professionals from the International Information Systems Security Certificate Consortium	MS, SC, and SE	MS influenced SC and information security policy enforcement.

Table continues.

Table 3 (Continued)

Study	Methodology	Sample	Instrument /Factor	Main Findings or Contribution
Knapp, Marshall, Rainer, and Ford (2007)	Interview and Survey	Interviews: 220 information security professionals from the International Information Systems Security Certification Consortium survey: 740 information security professionals from the International Information Systems Security Certification Consortium	MS, SA, SC, and SE.	MS positively influenced four variables of security effectiveness: user training, security culture, policy relevance, and policy enforcement. SA, and SC influenced SE.
Lineberry (2007)	Theoretical	Commentary	MS, SA, SC, and SE	SA training and social engineering testing affected security effectiveness. SE required a culture of information security awareness and management involvement.

Table continues.

Table 3 (Continued)

Study	Methodology	Sample	Instrument /Factor	Main Findings or Contribution
Madnick (1978)	Theoretical	Classical study	SE	The effectiveness of security countermeasures correlated to the risk of computer abuse occurrence.
Martin (1973)	Theoretical	Classical study	SE	The effectiveness of security countermeasures correlated to the risk of computer abuse occurrence.
Moreira, Martimiano, Brandão, and Bernardes (2008)	Theoretical	Commentary	SE	An information security governance framework enabled an effective information security management program.
Moynihan (2007)	Theoretical	Commentary	SA and SE	Employee security awareness training and the development of an ongoing security awareness program were central components of an effective information security strategy.

Table continues.

Table 3 (Continued)

Study	Methodology	Sample	Instrument /Factor	Main Findings or Contribution
Novakovic, McGill, and Dixon (2009)	Survey	111 computer users in Australia	Perceived usefulness of security, ease of use, facilitating conditions, secure behavior intention, and secure usage based on UTAUT	Facilitating conditions, ease of use, and experience influenced secure behavior intention. Secure behavior intention influenced secure usage in terms of effective password usage.
Pattinson and Anderson (2007)	Survey	Two pilot studies consisting of groups of 35 and 40 undergraduate students at the University of South Australia	SA, SE, and SB	User education and training, and understanding user behavior towards risk culture were needed to achieve an acceptable level of information security.
Pumphrey, Trimmer, and Beachboard (2007)	Theoretical	Commentary	SE	An effective information assurance program was needed to meet HIPAA security safeguard requirements.

Table continues.

Table 3 (Continued)

Study	Methodology	Sample	Instrument /Factor	Main Findings or Contribution
Rennie and Shore (2007)	Theoretical	Commentary	SE	A security framework, such as ISO/IEC 17799, increased the effectiveness of system security measures.
Smith and Jamieson (2006)	Discussion forum	11 representatives with technical and managerial backgrounds from 9 Australian government agencies	Security standards, MS, SA, and SE	Information security management standards, MS, and SA influenced SE and security compliance.
Straub (1990)	Survey	1211 IS directors, IS middle managers, IS security officers, controllers, and auditors from the Data Processing Management Association	MS and SE	A management decision to invest in IS security would result in more effective control of computer abuse.
Tang (2008)	Case study	A telecommunications marketing company in Taiwan	SA and SE	SA influenced SE.

Table continues.

Table 3 (Continued)

Study	Methodology	Sample	Instrument /Factor	Main Findings or Contribution
Tsohou, Kokolakis, Karyda, and Kiountouzis (2008)	Theoretical	MS, SA, SE, and SB	MS, SA, SE, and SB	MS affected SA, and SA influenced SE in the context of AMCs. SA influenced good end-user security behavior.
Winkel (2007)	Theoretical	Commentary	SA, SC, and SE	SA and SC significantly affected information security compliance and effective security management.

Management Support

Better understanding of management support for information security among AMCs is needed (Da Veiga & Eloff, 2007; Knapp & Boulton, 2006). According to McFadzean et al. (2007), "the roles and responsibilities of board members and senior executives for information security have received little attention in the academic literature to date" (p. 623). Many of the existing studies on the influence of top management support on technology adoption "suffer from diverse and inconsistent conceptual definitions, weak measures, and insufficient theorization" (Neufeld et al., 2007, p. 496). In addition, despite the increased media attention directed toward e-mail viruses, Internet worms, and software vulnerabilities, Chang and Ho (2006) and Knapp et al. (2006) determined that managers were not fully involved in ensuring security effectiveness.

Management Support Influence on Behavior

Management support is a major factor affecting secure compliance (Da Veiga & Eloff, 2007). Da Veiga and Eloff identified executive level sponsorship of information security and commitment from the board and management to protect information assets as critical information security components. Based on a study of 354 certified information security professionals who belonged to the International Information Systems Security Certificate Consortium, Ma et al. (2008) found that top management support was crucial in supporting security legislation such as the HIPAA Security Rule. Ma et al. determined that poor implementations of information security resulted from a "lack of authority, lack of executive support, and lack of understanding the importance of information security" (p. 265). Nevertheless, Da Veiga and Eloff determined that executive level management increasingly recognizes the value that information security brings to the organization.

Based on the results of a survey of IS managers, general managers, and chief executives of 505 companies in France, Bia and Kalika (2007) found that top management support positively influenced user security behavior toward regulatory requirements. Bia and Kalika determined that a standardized user code of conduct, as well as the use of general guidelines, caused users to better accept rules governing their behavior. This supported the claim of Jackson and Adams (1979), who asserted that standardization guaranteed stability and predictability of behavior.

According to Sveen et al. (2007), the management of secure information systems requires more than just a strong technical solution. Sveen et al. observed that, unless management demonstrates a total commitment and leads by example, subordinate staff will not follow. Similarly, Ma et al. (2008) reported that information security is more of a

"human" problem rather than a pure "technical" problem. The authors stated that human related problems are found in all levels of the organization, ranging from uninformed end users to ambivalent upper management. Da Veiga and Eloff (2007) noted that, "if management trusts its employees and the employees trust management, it is easier to implement new procedures and guide employees through changes of behavior pertaining to information security" (p. 367).

Management Support Influence on Security Effectiveness

Management support is important to achieving security effectiveness (Chang & Ho, 2006; Chang & Yeh, 2006). Knapp et al. (2007) used a sequential qualitative-quantitative methodological approach to propose a theoretical model regarding the role of top management support of information security effectiveness. The authors determined that top management support positively influenced four variables of security effectiveness: user training, security culture, policy relevance, and policy enforcement. Knapp et al. concluded that top management should "act as a champion of change in creating an organizational environment conducive to security goals" (p. 52).

In a study of 11 representatives with technical and managerial backgrounds from nine Australian government agencies, Smith and Jamieson (2006) investigated the key drivers and inhibitors affecting IS security success and security compliance. Smith and Jamieson determined that the active support of senior management was found to be the highest driver essential for effective security. According to the authors, this finding demonstrated that, although IS security concerns have been recognized by the IT department for many years, senior management had yet to fully appreciate the importance of IS security processes within the business framework. Of the key inhibitors, Smith and Jamieson

found that a lack of management awareness was the highest-ranking inhibitor, thus showing that information as an important resource needs to be acknowledged not only by staff but also by senior management.

Based on the results of a multi-case study, Loghry and Veach (2009) observed that senior management support and personal participation were critical for securing corporate assets and maintaining an effective risk management program. According to Loghry and Veach, “only the senior management of an organization can determine which threats are tolerable and which must be addressed immediately based on the organization's mission, goals, strategic plan, and budget” (p. 33). In a prior study, Knapp et al. (2007) argued that, “without management’s visible support, running an effective security program will be an uphill battle” (p. 34). Figure 6 presents Knapp et al.’s theoretical model depicting the relationships between top management support, user training, security culture, and security effectiveness.

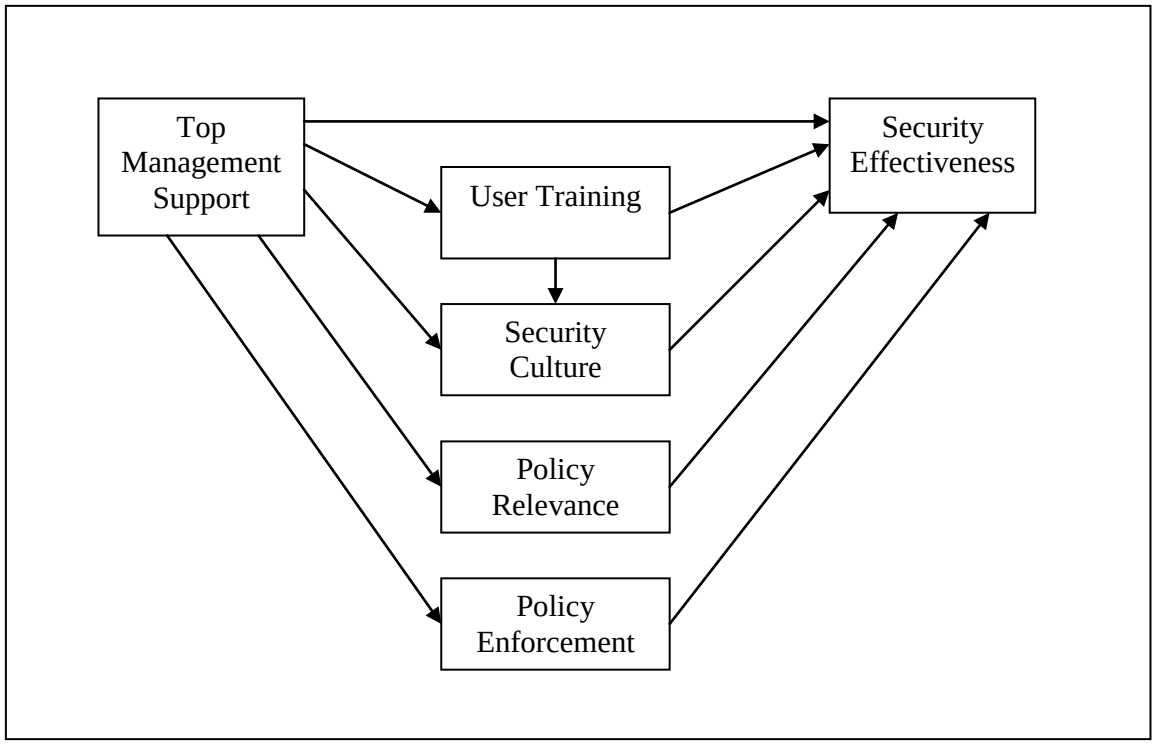

Figure 6. Theoretical model showing the relationships between top management support, user training, security culture, and security effectiveness (Knapp et al., 2007, p. 40).

Management Support Influence on Security Awareness

According to Casmir and Yngstrom (2005), effective security awareness requires first attracting the attention of senior executives toward a common understanding of the rationale for introducing security awareness programs. Swartz (2006) determined that a lack of security awareness training and difficulties experienced by hospital staff in complying with the HIPAA Security Rule was the result of several factors, one of which was a lack of senior management support. As indicated by Jennex (2007), good security awareness, a key component of all security programs, depends upon management support in generating, communicating, and implementing the security plan.

Based on a study of 144 business professionals, managers, IT administrators, and educators from various organizations, including health care, Rotvold (2008) found that:

> involving top management and getting their support is essential in building a strong security awareness program that employees will take seriously. If management commitment is increased, and the security awareness goals and message are communicated and communicated often, progress and improvement can be made in creating a security culture. (p. 38)

Management Support Influence on Security Culture

Top management support is a significant predictor of an organization's security culture (Knapp et al., 2006). Based on the results of an investigation of 220 certified information systems security professionals, Knapp et al. determined that low levels of executive support will produce an organizational culture less tolerant of good security practices as well as diminish the level of enforcement of existing security policies. Likewise, Chang and Lin (2007) found that managers should regard organizational culture as an important factor for supporting and guiding information security management practice. Chang and Lin concluded that organizational culture is "the media between management and organizational behavior, and different companies usually have different organizational cultures" (p. 439).

According to Da Veiga and Eloff (2007), information security culture develops in an organization due to certain actions taken by management and employees. The authors found that management influences information security culture by implementing policies and technical security measures. In addition, they found that employees interact with these information security components and exhibit behavior, such as the reporting of security incidents or sharing of passwords, which could either contribute or be a threat to the securing of information assets. As a result, Da Veiga and Eloff concluded that

executives are responsible for communicating the right information security culture and control framework and for exhibiting acceptable information security behavior.

A summary of the management support literature is presented in Table 4.

Table 4. Summary of the Management Support Literature

Study	Methodology	Sample	Instrument /Factor	Main Findings or Contribution
Bia and Kalika (2007)	Survey	IS managers, general managers, and chief executives of 505 companies in France	MS, SA, and SB	MS, user training, and security awareness campaigns positively influenced employee security behavior toward regulatory requirements.
Casmir and Yngstrom (2005)	Theoretical	Commentary	MS, SA, and SE	Effective security awareness programs required the attention of senior executives.
Chang and Ho (2006)	Survey	59 senior managers from various organizations, including health care	MS and SE	MS influenced SE.
Chang and Lin (2007)	Survey	108 senior IT managers and professionals from various industries, including health care	SC and MS on SE	Organizational culture and MS positively influenced information security management effectiveness.

Table continues.

Table 4 (Continued)

Study	Methodology	Sample	Instrument /Factor	Main Findings or Contribution
Chang and Yeh (2006)	Survey	109 managers of large Taiwan firms	SA, MS, and SE	SA and MS were required to reduce information security threats and achieve effective information security.
Da Veiga and Eloff (2007)	Theoretical	Commentary	MS, SA, SC, SB, and SE	MS and SA were needed for an acceptable level of information security culture and behavior.
Jackson and Adams (1979)	Theoretical	Commentary	MS	Management support for standardization guaranteed stable and predictable user behavior.
Knapp, Marshall, Rainer, and Ford (2006)	Survey	220 certified information systems security professionals from the International Information Systems Security Certificate Consortium	MS, SC, and SE	MS influenced SC and information security policy enforcement.

Table continues.

Table 4 (Continued)

Study	Methodology	Sample	Instrument /Factor	Main Findings or Contribution
Knapp, Marshall, Rainer, and Ford (2007)	Interview and Survey	Interviews: 220 information security professionals from the International Information Systems Security Certification Consortium survey: 740 information security professionals from the International Information Systems Security Certification Consortium	MS, SA, SC, and SE.	MS positively influenced four variables of security effectiveness: user training, security culture, policy relevance, and policy enforcement. SA, and SC influenced SE.
Loghry and Veach (2009)	Case study	A manufacturer, installer, and service provider of permanent and mobile lighting systems with global influence.	MS and SE	MS was positively correlated to an effective risk management program.

Table continues.

Table 4 (Continued)

Study	Methodology	Sample	Instrument /Factor	Main Findings or Contribution
Ma, Johnston, and Pearson (2008)	Survey	354 certified information security professionals from the International Information Systems Security Certificate Consortium	MS, SA, SC, SE, and SB.	MS influenced SA and HIPAA compliant information security behavior. SC, and organizational self-efficacy were positively correlated to effective information security management.
McFadzean, Ezingeard, and Birchall (2007)	Interviews	Forty-three interviews were conducted at executive level in 29 multi-national organizations	MS and SE	MS influenced effective security policies and information security strategies.
Neufeld, Dong, and Higgins (2007)	Survey	209 employees from seven mid-size-to-large Canadian manufacturing companies	MS and SB	MS influenced SB in the context of IT adoption and use behavior.

Table continues.

Table 4 (Continued)

Study	Methodology	Sample	Instrument /Factor	Main Findings or Contribution
Smith and Jamieson (2006)	Discussion forum	11 representatives with technical and managerial backgrounds from 9 Australian government agencies	Security standards, MS, SA, and SE	Information security management standards, MS, and SA influenced SE and security compliance.
Sveen, Rich, and Jager (2007)	Causal simulation study	Simulation model	MS, SA, SC, and SB	MS and SA influenced SC and SB.
Swartz (2006)	Theoretical	Commentary	MS and SA	SA and MS positively correlated to HIPAA security compliance.

Security Awareness

Tsohou et al. (2008) noted that information security awareness is "commonly regarded as aiming at improving information security by enhancing the adoption of security policies and countermeasures, improving IS users' security behavior, and altering work routine so that good security habits are applied" (p. 272). Despite the recent increased attention afforded to security incursions, Schmidt et al. (2008) contend that there is a lack of user awareness and understanding of information security. Thus, greater computer security awareness, education, and training in the context of AMCs is needed (Aytes & Connolly, 2004; Kruck & Teer, 2008; Wade, 2004).

According to Pattinson and Anderson (2007) and Winkel (2007), instead of addressing only the technical aspects of network security issues, attention needs to be paid to user awareness and behavior as a central focus of an information security strategy. For example, in a study examining encryption technologies at a university, Fritsche and Rodgers (2007) found the need to increase security awareness, offer additional security training, and provide solutions for e-mail encryption and digital signatures. Additionally, as indicated by Rotvold (2008), "all users should be aware not only of what their roles and responsibilities are in protecting information resources, but also of how they can protect information and respond to any potential security threat or issue" (p. 33).

Pfleeger and Rue (2008) found that regular testing and updating of security procedures, combined with practices that increase staff awareness, were critical to maintaining security. Additionally, Pfleeger and Rue noted that a lack of staff education and training within IT security teams and throughout the organization appeared to be a major obstacle to improved security. Williams (2008) reported that the increasingly electronic medical environment increasingly relies on general practitioners and staff who are not information security trained, thus creating considerable exposure of the medical practice. According to Williams, a more comprehensive and encompassing approach to security is required.

Security Awareness Influence on Security Compliance

Security awareness is a key factor in attaining HIPAA security compliance (Lending & Dillon, 2007; North et al., 2009). Touchet, Drummond, and Yates (2004) stated that providers' inadequate understanding of HIPAA negatively affects patient care. Wicke (2003) believes that HIPAA training should create awareness and educate users about

company policies and procedures addressing the regulations. As specified in the security and awareness training safeguards of the HIPAA Security Rule, health care organizations are required to take reasonable and appropriate steps to limit disclosure of PHI, including training employees, designating an individual with oversight, and securing access to ePHI (Medlin & Cazier, 2007).

To determine the key factors that enhance online learning effectiveness, Womble (2008) investigated 440 government agency employees in the southwestern U.S. The author found that mandatory training, such as that required by HIPAA, when taken online, improved employees' job performance and compliance with regulatory requirements. By requiring online training, managers were able to better track their employees' progress, increase employees' training satisfaction, lessen the amount of time needed for employees to complete the training, and increase organizational productivity (Womble). Similarly, Jarrell, Welker, Silsbee, and Tucker (2008) conducted an exploratory study of 80 students in a nursing school located in Central New York State and found that better delineation of training requirements by policy makers and the inclusion of clinical caregivers in developing the training materials and processes were needed.

Security Awareness and Social Engineering Influence on HIPAA Security Compliance

According to Lineberry (2007), two critical tools for fighting social engineering attacks are security awareness training and social engineering testing but that the effectiveness of these controls will vary based on the quality of their implementation, including follow-up and retraining. Kamal (2008) proposed a five-layer approach to prevent social engineering attacks, which includes developing an information security

policy, instituting security awareness, holding special training, implementing social engineering detection tools, and then repeating the aforementioned steps. In an empirical assessment of factors impeding effective password management, Medlin et al. (2008) determined that social engineering password attacks (social engineering is "the use of trickery, personal relationships, and trust to obtain information"), along with poor password creation and password sharing practices, were potential reasons for HIPAA security noncompliance (p. 72). The results of the Medlin et al. study raised "serious concerns about the state of employee security awareness" in health care organizations (p. 71).

Based on the findings of an investigation of 63 full-time health care workers from the University of Hartford in Connecticut, Kim (2005) found that the information security awareness levels of the respondents were not at an acceptable level due to a lack of ongoing security training. In a study of 90 employees in a single health care agency, Medlin and Cazier (2007) determined that more employee security training was needed to improve employee password selection procedures. These findings concur with those of Swartz (2006), who reported that sufficient security awareness training and budgeting for continued education and training is needed for HIPAA security compliance.

In a study of 355 undergraduate students at a large state university in the U.S., Kruck and Teer (2008) documented unsafe computer security practices. Kruck and Teer determined that increased security awareness training would have improved individual security practices. Schmidt et al. (2008) found that, despite the increased attention given to security vulnerabilities, "there appears to be a lack of user awareness and understanding of certain aspects of the security paradigm" (p. 91). Moreover, a study

conducted by the Verizon Business RISK team, concluded that “end-users proved to be the primary target of attacks employing deceit” and that “more effective security awareness programs at the end-user level” were needed (Baker et al., 2009, p. 25). Overall, there is a need for increased security awareness, education, and training (Dhillon & Blackhouse, 2001; Kirkpatrick, 2006; Leach, 2003; Siponen, 2000).

Security Awareness Influence on Secure Behavior

A variety of theories has been proposed for the study of security awareness, including social psychological theories such as social learning and instrumental learning (Thomson & von Solms, 1998) and motivational and behavioral theories such as TRA (Fishbein & Ajzen, 1975) and TPB (Ajzen, 1991). Through an extension of Ajzen’s TPB, Hazari et al. (2008) examined the factors influencing information security behavior, finding that attitudes, subjective norms, and perceived behavioral control (confidence) predict information security awareness. By understanding social cognition, organizations were found to be able to implement effective information security behavior (Hazari et al.).

Pattinson and Anderson (2007) noted that end user education and awareness training are two important human factors that have the potential to affect the security of an organization’s information systems. Filipek (2007) noted that 72% of organizations surveyed reported that training was the most effective means to change staff behavior and increase information security awareness. In an empirical study, Bia and Kalika (2007) determined that general guidelines taught through user training and security awareness campaigns are critical in maintaining stable and predictable employee behavior. Bia and Kalika found that “users also accept rules better when they are negotiated and introduced in a consensual way than when they are imposed from above” (p. 434).

Security Awareness Influence on Security Effectiveness

Since the proliferation of the microcomputer, employee training has been a recognized means of effective computer security (James, 1992). Given that every employee is part of the security team, a trained employee is an asset (Mitnick, 2003). Da Veiga and Eloff (2007) stated that user awareness, education, and training are critical information security components. Additionally, Hale and Brusil (2007) stated that, because a large part of security management must consider human vulnerability, enterprises must not overlook the importance of educating people about their personal role in providing and maintaining security. Security awareness, therefore, is an important determinant in achieving security effectiveness (D'Arcy & Hovav, 2009; Knapp et al., 2007).

As indicated by Moynihan (2007), employee awareness training is a central component of an effective information security strategy. An organization's most effective protection against employee security breaches is to "develop and implement a comprehensive system of internal controls that are integrated into an overall strategy of heightened security awareness and practice" (Alstete, 2006, p. 836). Chen, Shaw, and Yang (2006) determined that existing security problems were primarily due to the inadequate security awareness of users. They argued that effective information security awareness programs did not need sophisticated security technologies to mitigate internal or external security threats.

Chang and Yeh (2006) noted that effective information security should consider both technical and non-technical security threats. To address information threats, security awareness and security regulations should be reviewed to ensure a proper and secure

environment for a firm's information assets. Awareness of the required security principles according to specific IS/IT circumstances is fundamental to security (Chang & Yeh).

Based on their empirical investigation, Smith and Jamieson (2006) determined that awareness and training were key security issues in the implementation of information systems. They reported that awareness and training ranked fifth among key drivers of effective security. The authors concluded that awareness of information as an important resource needs to be recognized not only by staff but also by senior management.

Security Awareness Influence on Self-Efficacy

Awareness has been shown to be an important aspect of providing security (Goodhue & Straub, 1989; Im & Baskerville, 2005; Siponen, 2000; Straub & Welke, 1998). Goodhue and Straub (1991) were among the first IS scholars to suggest that awareness is an important factor in an individual's beliefs about information security. They predicted that computer abuse would be a major problem that would not diminish on its own and argued that "a lack of awareness of the danger may lead to weak vigilance by users and greater potential for abuse" (p.14). The authors argued that "people who are more aware of the potential for abuse would be sensitized to the dangers of inadequate security and would more likely feel that security was unsatisfactory" (p. 15). They concluded that awareness is related to computer literacy and defined an operationalized awareness as years of experience, managerial level, and user and systems staff status.

Security Awareness Influence on Security Culture and Management Support

In an empirical examination of information systems security issues of small business owners in Lynchburg, Virginia, Gupta and Hammond (2005) found that appropriate training and awareness within the organization are needed to foster a security culture.

Rotvold (2008) examined user perception of security awareness within organizations. Although most of the respondents in the Rotvold study reported that they were aware of the consequences for failing to comply with their organization's security policies, they also noted that incident response procedures were not well understood, security awareness goals were not measured or assessed, the effectiveness of the overall security awareness program was not evaluated or measured, and there was no assessment of security awareness or the information security program. According to Rotvold, identifying and communicating security awareness goals and messages, as well as repeating security messages often, were necessary to develop a security culture.

Further, Rotvold (2008) stated that involving top management and getting their support, as well as implementing social engineering testing, are essential requirements for building a strong security awareness program. A study by Casmir and Yngstrom (2005) identified a series of constraints and barriers to effective security awareness. According to these authors, addressing these factors requires attracting the attention of senior executives toward a common understanding of the rationale and importance of introducing security awareness programs. A summary of the security awareness literature is presented in Table 5.

Table 5. Summary of the Security Awareness Literature

Study	Methodology	Sample	Instrument /Factor	Main Findings or Contribution
Ajzen (1991)	Theoretical	Classical study	TPB, Attitude, Subjective Norm, and Perceived Behavioral Control, Behavioral Intention	Developed TPB as an extension of TRA. A user's behavior was determined by his or her intention to perform the behavior. Attitude toward the behavior, subjective norm, and perceived behavioral control were found to affect behavioral intention.
Alstete (2006)	Discussion forum	79 working professionals enrolled in three business course sections at a medium-sized college in the New York metropolitan area	SA, MS, and SE	SA and MS positively influenced SE in terms of preventing employee theft.
Aytes and Connolly (2004)	Survey	167 respondents at two large public universities	SA and computer policies and procedures	Computer security awareness, education, and training did not significantly alter the SB of users in regard to their use of computing practices.

Table continues.

Table 5 (Continued)

Study	Methodology	Sample	Instrument /Factor	Main Findings or Contribution
Baker, Hutton, Hylender, Novak, Porter, Sartin, et al. (2009)	Survey	90 data breach investigations that occurred in the U.S. in 2008	SA	Based on 285 million records being breached in 2008, SA programs were needed at the end-user level.
Bia and Kalika (2007)	Survey	IS managers, general managers, and chief executives of 505 companies in France	MS, SA, and SB	MS, user training, and security awareness campaigns positively influenced employee security behavior toward regulatory requirements.
Casmir and Yngstrom (2005)	Theoretical	Commentary	MS, SA, and SE	Effective security awareness programs required the attention of senior executives.
Chang and Yeh (2006)	Survey	109 managers of large Taiwan firms	SA, MS, and SE	SA and MS were required to reduce information security threats and achieve effective security.
Chen, Shaw, and Yang (2006)	Case study	Single insurance company that has an e-business function	SA and SE	Used the systems development research methodology. Effective system management components were critical for ensuring users gain adequate information security awareness.

Table continues.

Table 5 (Continued)

Study	Methodology	Sample	Instrument /Factor	Main Findings or Contribution
D'Arcy and Hovav (2009)	Survey	238 employed working professionals taking MBA classes at two mid-Atlantic U.S. universities	CSE, SA, IS misuse behavioral intention	CSE affected SA effectiveness and IS misuse behavioral intention in terms of unauthorized access and unauthorized modification.
Da Veiga and Eloff (2007)	Theoretical	Commentary	MS, SA, SC, SB, and SE	MS and SA were needed for an acceptable level of information security culture and behavior.
Dhillon and Blackhouse (2001)	Theoretical	Commentary	SA and SE	Identified the need for increased SA, education, and training in order to achieve effective security.
Filipek (2007)	Survey	Multiple organizations from Europe	SA and SE	Training was the most effective technique to change staff behavior and increase information security awareness.
Fishbein and Ajzen (1975)	Theoretical and survey	N/A	TRA constructs, including attitude toward behavior and subjective norm	Developed TRA. The most significant predictor of behavior was intention. Thus it was useful in describing behavior.

Table continues.

Table 5 (Continued)

Study	Methodology	Sample	Instrument /Factor	Main Findings or Contribution
Fritsche and Rodgers (2007)	Case study	Single university in the U.S.	SA	Increased security awareness, additional security training, and security solutions for e-mail encryption, digital signatures, and mobile device removable media was needed.
Goodhue and Straub (1989)	Theoretical and survey	Randomly selected Data Processing Management Association members	SA	Awareness was an important step to providing security.
Goodhue and Straub (1991)	Theoretical and survey	570 randomly selected Data Processing Management Association members and 357 end-users.	SA and human behavior	Awareness and human behavior were important factors affecting an individual's view of information security.
Gupta and Hammond (2005)	Survey	138 small business owners in Lynchburg, Virginia	MS, SA, and SC	MS and SA were positively correlated to fostering a security culture.
Hale and Brusil (2007)	Theoretical	Commentary and 15-year historical perspective of security management	SA	Educating people about their personal role in providing and maintaining security was critical for security management.

Table continues.

Table 5 (Continued)

Study	Methodology	Sample	Instrument /Factor	Main Findings or Contribution
Hazari, Hargrave, and Clenney (2008)	Survey	179 undergraduate and graduate business school students in a state university in the southeastern U.S.	Attitudes, subject norm, and perceived behavioral control, (CSE) on SA, SE, and SB	Social cognition factors, such as attitude, subject norm, and perceived behavioral control influenced SA and information security behavior effectiveness.
Im and Baskerville (2005)	Theoretical and longitudinal study	1993 original study and 2005 replicated study	SA	Security awareness training should be promoted as important elements of organizational security programs.
James (1992)	Theoretical	Classical study	SA	Employee training influences effective computer security.
Jarrell, Welker, Silsbee, and Tucker (2008)	Survey	80 students in a School of Nursing located in Central New York State	SA, SC, and SE	SA and SC influenced effective security in terms of flow of services, patient satisfaction, health care team satisfaction, and quality of care.
Kamal (2008)	Theoretical	Commentary	SA	SA was needed to prevent social engineering security threats.

Table continues.

Table 5 (Continued)

Study	Methodology	Sample	Instrument /Factor	Main Findings or Contribution
Kim (2005)	Survey	63 full time health care workers from the University of Hartford in Connecticut	SA and SB	Ongoing security training was required for acceptable levels of SA.
Kirkpatrick (2006)	Theoretical	Commentary	SA	There was a need for increased SA.
Knapp, Marshall, Rainer, and Ford (2007)	Interview and Survey	Interviews: 220 information security professionals from the International Information Systems Security Certification Consortium survey: 740 information security professionals from the International Information Systems Security Certification Consortium	MS, SA, SC, and SE.	MS positively influenced four variables of security effectiveness: user training, security culture, policy relevance, and policy enforcement. SA, and SC were found to influence SE.

Table continues.

Table 5 (Continued)

Study	Methodology	Sample	Instrument /Factor	Main Findings or Contribution
Kruck and Teer (2008)	Survey	355 undergraduate students at one large state university on the east coast	SA on SB	SA influenced individuals' security practices.
Leach (2003)	Theoretical	Commentary	SA	There was a need for increased security awareness, education, and training.
Lineberry (2007)	Theoretical	Commentary	MS, SA, SC, and SE	SA training and social engineering testing affected security effectiveness. SE required a culture of information security awareness and management involvement.
Medlin and Cazier (2007)	Survey	90 employees of a health care agency	SA on SB	SA influenced SB.
Medlin, Cazier, and Foulk (2008)	Survey	118 employees from 5 hospitals	SA and SB	SA influenced SB.
Mitnick (2003)	Theoretical	Commentary	SA	A lack of employee security awareness increased security risk levels.

Table continues.

Table 5 (Continued)

Study	Methodology	Sample	Instrument /Factor	Main Findings or Contribution
Moynihan (2007)	Theoretical	Commentary	SA and SE	Employee security awareness training and the development of an ongoing security awareness program were central components of an effective information security strategy.
North, North, and North (2009)	Theoretical	Commentary	SA	User security training and education influenced HIPAA security compliance.
Pattinson and Anderson (2007)	Survey	Two pilot studies consisting of groups of 35 and 40 undergraduate students at the University of South Australia	SA, SE, and SB	User education and training, and understanding user behavior towards risk culture were needed to achieve an acceptable level of information security.
Pfleeger and Rue (2008)	Survey	Multiple survey samples	SA and SC	SA influenced SC.

Table continues.

Table 5 (Continued)

Study	Methodology	Sample	Instrument /Factor	Main Findings or Contribution
Rotvold (2008)	Survey	144 business professionals, managers, IT administra-tors, and educators from various organizations, including health care	MS, SA, SC, and SE	MS influenced SA, and that SA influenced SC and information security program effectiveness.
Schmidt, Johnston, Arnett, Chen, and Li (2008)	Survey	210 U.S. students from three public colleges in various geographic regions, and 278 Chinese college students in China	SA, SC, and SE	SA and SC influenced SE.
Siponen (2000)	Theoretical	Commentary	SA	SA influenced information security behavior.
Smith and Jamieson (2006)	Discussion forum	11 representatives with technical and managerial backgrounds from 9 Australian government agencies	Security standards, MS, SA, and SE	Information security management standards, MS, and SA influenced SE and security compliance.

Table continues.

Table 5 (Continued)

Study	Methodology	Sample	Instrument /Factor	Main Findings or Contribution
Straub and Welke (1998)	Comparative qualitative studies	Interviewed 37 management at various levels over 15-month period in a fortune 500 company, as well as executive management over a 4-month period in another fortune 500 company	SA, risk analysis, security problem resolution	Developed a security program that included the use of a security risk planning model, education and training in security awareness, and countermeasure matrix analysis. SA influenced effective security.
Thomson and von Solms (1998)	Theoretical	Commentary	SA	Proposed the social learning and instrumental learning theory to explain the importance of security awareness.
Touchet, Drummond, and Yates (2004)	Theoretical	Commentary	SA	An inadequate understanding of HIPAA regulations negatively affected patient care.
Tsohou, Kokolakis, Karyda, and Kiountouzis (2008)	Theoretical	Commentary	MS, SA, SE, and SB	MS affected SA, and SA influenced SE in the context of AMCs. Also SA influenced good end-user security behavior.

Table continues.

Table 5 (Continued)

Study	Methodology	Sample	Instrument /Factor	Main Findings or Contribution
Wade (2004)	Theoretical	Commentary	SA	There was a need to require the individual to assume more responsibility regarding computer security.
Wicke (2003)	Theoretical	Commentary	SA	SA positively correlated to HIPAA security compliance.
Williams (2008)	Theoretical	Commentary	SA	A security operational framework, such as SSE-CMM, was useful in improving medical practice security requirements. Increased security training was needed in health care environments.
Winkel (2007)	Theoretical	Commentary	SA, SC, and SE	SA and SC significantly affected information security compliance and effective security management.
Womble (2008)	Survey	440 government agency employees in the southwestern U.S.	SA, CSE, and SB	CSE was a significant predictor of security compliance behavior. a positive relation existed between self-efficacy and two variables: satisfaction and perceived usefulness.

Security Culture

More attention needs to be paid to the information security culture of AMCs (Da Veiga & Eloff, 2007; Von Solms, 2000). According to Beatson (1991), "within the corporate culture, security should be given prominence. Because security involves people, it is also very important that other elements within the corporate culture are recognized" (p. 30). Siponen (2001), however, stated that very little research has been undertaken on the socio-technical aspects of information security. In an investigation by Ma et al. (2008), information security and computer security were reported to be often implemented as an afterthought. Because time, compromise, and painful experiences are required for an organization to establish and enforce security policies, the authors concluded that critical factors such as organizational culture and policy would have a significant effect on the success on information security management

According to Guzman et al. (2008), additional research on the social and cultural aspects of employees' workplace interactions with each other and with technology is needed. The authors determined that organizational culture includes many complex and varying facets, such as leadership styles, strategies for organizational change, knowledge management, and general management styles within organizations as well as human resource strategies to achieve organizational performance. Guzman et al. concluded that IT personnel have established a distinct occupational culture within organizations, characterized by (a) the use of technical jargon; (b) valuing technical knowledge; (c) extreme and unusual demands based on constant change; (d) feelings of superiority; and (e) a general lack of formal rules. They concluded that organizational sub-cultures caused conflict and affected compliance behavior within different departments.

Security Culture Influence on Security Compliance

Security culture has been found to play a significant role in information security compliance (Ma et al., 2008). Winkel (2007) defined security culture as "the system of collective moral concepts, mindsets and behavior patterns anchored in the self-conception of a social unit and instructing its members in dealing with security threats" (p. 223). According to Huebner and Britt (2006), a culture of security refers to "a focus on security in the development of information systems and networks and the adoption of new ways of thinking and behaving when using and interacting within information systems and networks" (Organization for Economic Cooperation and Development, 2002, p. 8). In addition, an empirical investigation by Rotvold (2008) reported that security culture was determined to exert a positive influence on security compliance.

Security Culture Influence on Security Behavior

According to Leidner and Kayworth (2006), "culture is a critical variable in explaining how social groups interact with IT" (p. 360). Deal and Kennedy (1982) noted that culture is the single most important factor accounting for the success or failure of an organization. Schein (1999) reported that "culture matters because it is a powerful, latent, and often unconscious set of forces that determine both our individual and collective behavior, ways of perceiving, thought patterns, and values" (p. 14). Schein observed that organizations develop powerful cultures that guide the thinking and behavior of their employees.

When applied to the implementation of new systems and processes, organizational culture is a key organizational component (Mills, Platts, & Gregory, 1995). Kennerley and Neely (2002) found inappropriate organizational culture, ineffective processes and

the lack of skills to be important barriers to systems evolution. In this regard, initiatives for adopting new information technology frequently experienced difficulties because people were hesitant to change what they were used to and lacked the motivation to change their habits (Allen & Fifield, 1999; Cooper, 2000).

Security Culture Influence on Security Effectiveness

Organizational culture is defined as the:

> pattern of shared basic assumptions that the group learned as it solved its problems of external adaptations and internal integrations that has 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. (Schein, 1992, p. 12)

Ruighaver and Maynard (2006) stated that security culture is based on an organizational culture framework.

Chan et al. (2005) referred to organizational culture as the "values, beliefs and assumptions found in the deep structure of organizations, which are held by its members" (p. 20). The authors observed that compliant behavior can be increased by enhancing employees' perception of information security climate. They identified coworker socialization, direct supervisory practices, and upper management practices as factors that positively affected information security climate.

Alstete (2006) investigated the perceptions of current and previous employees in regard to detecting and preventing employee theft. According to the employees, a company's most effective protection against loss from employees was to have a comprehensive system of internal controls that are integrated into an overall strategy of heightened security awareness and practice. This comprehensive strategy should include

a culture of honesty with a written code of ethics and conduct, proper employee screening, background checks, technology measures, careful inventory control, and overall continued awareness and vigilance by management (Alstete). In an empirical investigation, Chang and Lin (2007) examined the influence of organizational culture on the implementation of information security management. They sought to determine how organizational culture influenced information security management effectiveness, to explain the relationships between organizational culture traits and information security management principles, and to identify the kind of culture conducive to information security management implementation. The authors derived four regression models to quantify the impact of organizational culture traits on the effectiveness of information security management.

Based on their findings, Chang and Lin (2007) reported that control-oriented organizational culture traits, such as effectiveness and consistency, have a strong effect on the information security management principles of confidentiality, integrity, availability, and authentication. They also noted that the flexibility-oriented organizational culture traits, such as cooperativeness and innovativeness, are not significantly associated with the information security management principles. The authors concluded that an appropriate and effective information security management implementation requires a combination of favorable organizational culture, competent information security technology, and management's supportive attitude toward information security.

According to Winkel (2007), a security culture can be understood equally as the basis and result of security management and stated that a rational design of security processes

is required for effective security management, which should be grounded in an appropriate security culture. Winkel's investigation validated prior studies by Dhillon (2001) and Winkel (2001), which came to the same conclusion.

Security Culture Influence on Security Awareness

Gupta and Hammond (2005) believe that a security culture is fostered by the implementation of a comprehensive solution that includes physical, procedural, and logical forms of protection, along with the appropriate training and awareness within the organization. Based on a study investigating the effects of outsourcing information security, Karyda, Mitrou, and Quirchmayr (2006) found that total security outsourcing caused a decrease in the development of a security culture within the organization. They also found that employees lacked awareness of security related issues. The authors thus concluded that a minimum level of information security experience and expertise be maintained within the organization.

Lineberry (2007) reported that effective information security must be culturally ingrained and backed by strategies and processes that are continually tested, taught, measured, and refined. To foster a culture that is information security aware, Lineberry believes that company management should ask the following questions:

1. Are employees educated about and aware of common information security threats?

2. Do they write down or freely share passwords with others?

3. Do visitors freely move about facilities without facing barriers to entry, such as a requirement to wear a company-issued badge?

4. Is it common to see sensitive information, such as completed employment applications or client documents containing Social Security numbers, accessible in unmonitored or otherwise unsecured areas?

5. What is the prevailing employee attitude regarding information security controls?

6. Are enforced information controls viewed primarily as a nuisance or a necessity?

A summary of the security culture literature is presented in Table 6.

Table 6. Summary of the Security Culture Literature

Study	Methodology	Sample	Instrument /Factor	Main Findings or Contribution
Allen and Fifield (1999)	Theoretical and case study	Five universities in the U.S.	Culture	IT adoption rates were impeded due to user-related resistance to change and lack of motivation to change existing habits.
Alstete (2006)	Discussion forum	79 working professionals enrolled in three business courses at a medium-sized college in the New York metropolitan area	SA, MS, and SE	SA and MS positively influenced SE in terms of preventing employee theft.
Beatson (1991)	Theoretical	Commentary	SC	Security should be given prominence with the corporate culture.

Table continues.

Table 6 (Continued)

Study	Methodology	Sample	Instrument /Factor	Main Findings or Contribution
Chan, Woon, and Kankanhalli (2005)	Survey	104 employees from two IT intensive organizations in the logistics and petrochemical industries	Information security climate, self-efficacy, MS, and compliant behavior	Coworker socialization, direct supervisory practices, and upper management practices affected information security climate. Information security climate and self-efficacy influenced compliant behavior.
Chang and Lin (2007)	Survey	108 senior IT managers and professionals from various industries, including health care	SC and MS on SE	Organizational culture and MS positively influenced information security management effectiveness.
Da Veiga and Eloff (2007)	Theoretical	Commentary	MS, SA, SC, SB, and SE	MS and SA were needed for an acceptable level of information security culture and behavior.
Deal and Kennedy (1982)	Theoretical	Classical study	SC	Culture was the single most important factor accounting for success or failure of an organization.
Dhillon (2001)	Theoretical	Commentary	SC	Effective security processes require a sustainable security culture.

Table continues.

Table 6 (Continued)

Study	Methodology	Sample	Instrument /Factor	Main Findings or Contribution
Gupta and Hammond (2005)	Survey	138 small business owners in Lynchburg, Virginia	MS, SA, and SC	MS and SA were positively correlated to fostering a security culture.
Guzman, Stam, and Stanton (2008)	Semi-structured interviews	32 IT personnel and 89 other employees from eight non-profit organizations, including a university and hospital	SC and SB	Organizational and occupational culture positively influence HIPAA security compliant behavior in AMCs.
Huebner and Britt (2006)	Theoretical	Commentary	SC and SB	The cultural aspects of an enterprise were vital to the success of a security program. Behavioral aspects of security, such as emotional intelligence, structural theory, and social network analysis, influence enterprise security.
Karyda, Mitrou, and Quirchmayr (2006)	Theoretical	Commentary	SA and SC	Security outsourcing Negatively influenced SC. A lack of SA negatively affected security levels.

Table continues.

Table 6 (Continued)

Study	Methodology	Sample	Instrument /Factor	Main Findings or Contribution
Kennerley and Neely (2002)	Theoretical and case study	Seven companies from various industry sectors	Culture	Inappropriate organizational culture was an important barrier to systems evolution.
Leidner and Kayworth (2006)	Theoretical	Commentary	Culture	Culture was a critical variable in explaining how social groups interact with IT.
Lineberry (2007)	Theoretical	Commentary	MS, SA, SC, and SE	SA training and social engineering testing affected security effectiveness. SE required a culture of information security awareness and management involvement.
Ma, Johnston, and Pearson (2008)	Survey	354 certified information security professionals from the International Information Systems Security Certificate Consortium	MS, SA, SC, SE, and SB.	MS influenced SA and HIPAA compliant information security behavior. Organizational self-efficacy was positively correlated to effective information security management.

Table continues.

Table 6 (Continued)

Study	Methodology	Sample	Instrument /Factor	Main Findings or Contribution
Mills, Platts, and Gregory (1995)	Theoretical	Commentary	Culture	Organizational culture can be a key organizational constraint in implementing new systems and processes.
Rotvold (2008)	Survey	144 business professionals, managers, IT administra-tors, and educators from various organizations, including health care	MS, SA, SC, and SE	MS influenced SA, and SA influenced SC and information security program effectiveness.
Ruighaver and Maynard (2006)	Theoretical	Commentary	SC	A security culture was based on an organizational culture framework.
Schein (1992)	Theoretical	Commentary	Organizational culture	Culture needs to be taught to new employees to enable the correct way to perceive, think, and feel in relation to those problems.
Schein (1999)	Theoretical	Commentary	Culture	Culture had an unconscious influence on organizational behavior.

Table continues.

Table 6 (Continued)

Study	Methodology	Sample	Instrument /Factor	Main Findings or Contribution
Siponen (2001)	Theoretical	Commentary	SC	Additional research on the socio-technical aspects of information security was needed to increase organizational security culture.
Von Solms (2000)	Theoretical	Commentary	MS and SC	Increased attention was needed for organizational information security culture. MS participation influenced organizational security levels. Trust was a critical issue in establishing information security in an IT environment.
Winkel (2001)	Theoretical	Commentary	SC	Effective security processes require a sustainable security culture.
Winkel (2007)	Theoretical	Commentary	SA, SC, and SE	SA and SC significantly affected information security compliance and effective security management.

Computer Self-Efficacy

Research on the factors associated with self-efficacy in AMCs is warranted (Ball & Levy, 2008; Lending & Dillon, 2007). According to Lending and Dillon, "the self-efficacy of nurses and their perceptions of data security and confidentiality are relatively unknown" (p. 52). Moreover, Womble (2008) concluded that the literature has shown that users with high information and self-efficacy will perceive IT as a useful and resourceful tool and will, therefore, remain compliant with federal and state requirements. According to Ma et al. (2008), organizational self-efficacy is a critical success factor of information security management (levels and practices) and thus HIPAA compliance.

Bandura (1986) defined self-efficacy as:

> people's judgments of their capabilities to organize and execute courses of action required to attain designated types of performances. It is concerned, not with the skills one has, but with judgments of what one can do with whatever skills one possesses. (p. 391)

Lending and Dillon (2007) provided a related definition, stating that self-efficacy refers to "a user's confidence that he or she has the ability to use an information system" (p. 50). Extending the self-efficacy construct to computer usage, Compeau and Higgins (1995) defined computer self-efficacy as "a judgment of one's capability to use a computer" (p. 192). Computer self-efficacy is an important determinant of security compliance behavior (Chan et al., 2005; Lending & Dillon; Womble, 2008). In this regard, Langford and Reeves (1998) reported that individuals with high computer self-efficacy showed confidence in their ability to control their fate when using computers.

Further, Compeau and Higgins (1995) found that those who were confident developed even higher computer self-efficacy levels with continued computer use.

Self-Efficacy Influence on Security Behavior

Self-efficacy is a valid predictor of information security behavior (Chan et al., 2005). Chan et al. reported that self-efficacy positively influenced employees' compliant behavior and that "compliant behavior is dependent on a combination of organizational and personal factors" (p. 36). The authors also stated that "compliant behavior can be promoted by increasing employees' self-efficacy and enhancing perception of information security climate" (p. 36).

According to Compeau and Higgins (1995), researchers generally agreed that a positive relationship existed between CSE and IS use, and that understanding CSE was important to the successful implementation of systems in organizations. In a later study, Compeau, Higgins, and Huff (1999) empirically validated the CSE instrument confirmed in their prior work. The results of the Compeau et al. study provided strong confirmation and evidence that CSE affects an individual's affective and behavioral reactions to IS. Agarwal and Karahanna (2000) observed that an individual's beliefs about or perceptions of IS have a significant influence on their usage behavior. Agarwal and Karahanna's study also concurred with the results of Dinev & Hart (2006), which demonstrated that people with low levels of computer self-efficacy tended to avoid technology and have anxiety towards technology.

In an exploratory study of 179 undergraduate and graduate business school students in a state university in the southeastern U.S., Hazari et al. (2008) examined the perceptions of users on the requirements in personal firewall software. The authors extended Ajzen's

TPB to predict information security awareness and behavior. Hazari et al. observed that intention to maintain information security behavior could be predicted by the confidence (self-efficacy) of their participants.

Self-Efficacy Influence on Security Awareness

In an empirical study, Womble (2008) found that there were significant positive correlations between e-learning self-efficacy and e-learning satisfaction and perceived usefulness. These results suggest that employees who believe that taking mandated online training (e.g., HIPAA) would improve their job performance were also satisfied with the training. By placing mandated training online, Womble noted that managers can not only track their employees' progress easily but also keep a record of their own compliance with state and federal laws.

Womble (2008) also determined that, if employees were satisfied with online learning, they may be more inclined to complete the course, which, in turn, would keep their organizations in compliance with regulatory requirements. As a result, Womble suggested that organizations administer evaluation surveys to assess employees' self-efficacy and satisfaction levels to ensure compliance with mandated training program requirements. Womble's findings concurred with the prior research of Compeau and Higgins (1995) and Compeau et al. (1999), which showed that end users with high information will stay compliant with federal and state training mandates and users with high self-efficacy will perceive information technology as a useful and resourceful tool.

Hazari et al. (2008) used confidence in maintaining information security as an aspect of perceived behavioral control. Perceived behavioral control is similar to Bandura's concept of self-efficacy and was derived from the TPB. Consequently, Hazari et al. found

that attitudes, subjective norms, and perceived behavioral control (confidence) were related to maintaining information security awareness. Hazari et al. concluded that, by understanding social cognition, organizations can better teach employees about effective information security behavior.

Self-Efficacy Influence on Data Security Breaches

In a study of 82 undergraduate students from the College of Business Administration at a central Texas university, White et al. (2008) determined that unauthorized secondary use of personal data and concern for collection of personal data had a significant relationship with computer self-efficacy. The authors found that "a higher level of computer self-efficacy (confidence with the computer technology) may result in a lower level of concern for information privacy (management of the information)" (p. 70). This was in keeping with the research of Rifon, LaRose, and Choi (2005), who determined that users with high computer self-efficacy showed greater trust with increased technology. Additionally, in an empirical investigation of 324 students, Havelka (2003) reported that users with lower levels of computer abuse had higher levels of computer self-efficacy.

D'Arcy and Hovav (2009) noted that research on computer self-efficacy suggests that there is a significant relationship between perceptions of self-efficacy and risk-taking behavior. In their investigation of 238 working professionals taking MBA classes at two mid-Atlantic U.S. universities, D'Arcy and Hovav found that computer self-efficacy negatively influenced the relationship between user awareness of security countermeasures and IS misuse intention. Users with higher computer self-efficacy (computer-savvy individuals) tended to ignore security awareness programs and

computer monitoring due to the belief that they would be less likely to be caught if engaged in an unauthorized activity (D'Arcy & Hovav). According to the authors, security education and training programs should take into consideration employees' level of computer understanding. Similarly, the moderating effect of computer self-efficacy on monitoring suggests that users with more computer knowledge believe that they can "cheat" the system and avoid the implications of monitoring technologies. Thus, when implementing such technologies, organizations need to convey to computer-savvy users that they are not immune (D'Arcy & Hovav).

A summary of the computer self-efficacy literature is presented in Table 7.

Table 7. Summary of the Computer Self-Efficacy Literature

Study	Methodology	Sample	Instrument /Factor	Main Findings or Contribution
Agarwal and Karahanna (2000)	Survey	288 students enrolled in a junior level statistics class	CSE, behavioral intention, and perceived ease of use	An individual's beliefs about or perceptions of IS have a significant influence on their usage behavior.
Ball and Levy (2008)	Survey	111 instructors teaching IS and non-IS courses at a small private university in the southeastern U.S.	CSE, computer abuse, and experience with the use of technology on intention to use	Only CSE influences intention to use and behavior.
Bandura (1986)	Theoretical	Classical study	CSE and SB	Developed social cognitive theory to address technology acceptance.
Chan, Woon, and Kankanhalli (2005)	Survey	104 employees from two IT intensive organizations in the logistics and petrochemical industries	Information security climate, self-efficacy, MS, and compliant behavior	Coworker socialization, direct supervisory practices, and upper management practices affected information security climate. Information security climate and self-efficacy influenced compliant behavior.

Table continues.

Table 7 (Continued)

Study	Methodology	Sample	Instrument /Factor	Main Findings or Contribution
Compeau and Higgins (1995)	Survey	1,020 knowledge workers	CSE	Individuals who were confident developed increased CSE levels with continued computer use.
Compeau, Higgins, and Huff (1999)	Theoretical and survey	2,000 subscribers to a Canadian periodical	CSE, outcome expectations, affect, anxiety, and usage	CSE influenced user affective and behavioral reactions to IT.
D'Arcy and Hovav (2009)	Survey	238 employed working professionals taking MBA classes at two mid-Atlantic U.S. universities	CSE, SA, IS misuse behavioral intention	CSE affected SA effectiveness and IS misuse behavioral intention in terms of unauthorized access and unauthorized modification.
Dinev and Hart (2006)	Survey	422 respondents	CSE and SB	Examined Internet privacy concerns and user behavior intentions. Users with low levels of CSE tended to avoid technology and exhibit anxiety towards technology.
Havelka (2003)	Survey	324 undergraduate business students	CSE	Users with lower levels of computer abuse had higher levels of computer self-efficacy.

Table continues.

Table 7 (Continued)

Study	Methodology	Sample	Instrument /Factor	Main Findings or Contribution
Hazari, Hargrave, and Clenney (2008)	Survey	179 undergraduate and graduate business school students in a state university in the southeastern U.S.	Attitudes, subject norm, and perceived behavioral control, (CSE) on SA, SE, and SB	Social cognition factors, such as attitude, subject norm, and perceived behavioral control influenced SA and information security behavior effectiveness.
Langford and Reeves (1998)	Survey	127 upper-division university business students	CSE	Individuals with high CSE showed confidence in their ability to control their fate when using computers.
Lending and Dillon (2007)	Survey	139 nursing staff members from a single hospital	SA, MS, and CSE	SA and MS influenced self-efficacy and HIPAA compliance.
Ma, Johnston, and Pearson (2008)	Survey	354 certified information security professionals from the International Information Systems Security Certificate Consortium	MS, SA, SC, SE, and SB.	MS influenced SA and HIPAA compliant information security behavior. Organizational self-efficacy was positively correlated to effective information security management.

Table continues.

Table 7 (Continued)

Study	Methodology	Sample	Instrument /Factor	Main Findings or Contribution
Rifon, LaRose, and Choi (2005)	Survey	210 undergraduate students at a major Midwestern university	CSE	Users with high computer self-efficacy showed greater trust with increased technology.
White, Shah, Cook, and Mendez (2008)	Survey	82 undergraduate students from the College of Business Administration at a central Texas university	CSE, unauthorized secondary use, and improper access	CSE influenced unauthorized secondary use but not improper access.
Womble (2008)	Survey	440 government agency employees in the southwestern U.S.	SA, CSE, and SB	CSE was a significant predictor of security compliance behavior. A positive relation existed between self-efficacy and two variables: satisfaction and perceived usefulness.

Summary of What is Known and Unknown About the Topic

This chapter presented a review and analysis of the body of literature specific to the constructs of the investigation. To study the factors that affect HIPAA security compliance in AMCs, the author developed a research framework by conducting a literature search in a broad variety of fields, including IS security, sociology and psychology, management science, and organizational behavior. The literature related to

the HIPAA Security Rule also was reviewed. According to Helms et al. (2008), the HIPAA Security Rule is a significant regulation affecting health care organizations. Growing numbers of data security breach incidents (Gallagher, 2009), increased security requirements resulting from expanding IT infrastructure (Pirim et al., 2008), stricter enforcement of the HIPAA Security Rule (Hourihan, 2009), and extended HIPAA Security Rule requirements (Aguilar, 2009) have become important concerns in health care.

The author reviewed the literature on the constructs of security behavior, security effectiveness, management support, security awareness, security culture, and computer self-efficacy in the context of the larger construct of information security knowledge. A review of the technology acceptance literature was completed as a means to understand security behavior (Dinev & Hu, 2007). This included TRA (Ajzen & Fishbein, 1980), TPB (Ajzen, 1985), TAM (Davis, 1989), TAM2 (Venkatesh & Davis, 2000), and UTAUT (Venkatesh et al., 2003). Security behavior was found to be a key factor affecting health care organizations' security effectiveness and HIPAA security compliance (Chan et al., 2005; Johnston & Warkentin, 2008; Novakovic et al., 2009); and security effectiveness was found to be a key construct affecting security behavior and HIPAA security compliance in health care (Chang & Lin, 2007; D'Arcy & Hovav, 2009; Hazari et al., 2008).

The variables of management support, security awareness, security culture, and computer self-efficacy were determined to affect security behavior and security effectiveness and thus HIPAA security compliance in AMCs (D'Arcy & Hovav, 2009; Da Veiga & Eloff, 2007; Ma et al., 2008; Thomas & Botha, 2007; Womble, 2008). Based

on the gaps in the literature, the author will conduct an empirical investigation to develop and validate a model for predicting the effect of management support, security awareness, security culture, and computer self-efficacy on security behavior and security effectiveness and thus HIPAA security compliance in AMCs.

Contribution this Study Makes to the Field

The contributions of this investigation are several. First, the main contribution of this study is to provide an understanding of the key factors that affect HIPAA security compliance in AMCs. Literature on HIPAA security and information security has identified a number of factors that contribute to security behavior and security effectiveness, including management support (Barry & Grossmeier, 2009), security awareness (Lending & Dillon, 2007), security culture (Ma et al., 2008), and computer self-efficacy (Chan et al., 2005). Additionally, security effectiveness (D'Arcy & Hovav, 2009) and security behavior (Keith et al., 2009) were found to be valid predictors of each other as well as of HIPAA security compliance (Chang & Ho, 2006; Johnston & Warkentin, 2008; Rotvold, 2008). Understanding these factors is expected to facilitate the understanding of HIPAA security compliance among AMCs (Lawrence, 2007).

Second, understanding and addressing relevant security-related concerns remains a top priority in AMCs. According to Herod (2009b), data security breaches in health care organizations continue to increase. Numerous AMCs reported data security breaches in 2009 and 2010 (DataLossDB, 2010; Privacy Rights Clearinghouse, 2010). Slow IT adoption has been an internal weakness in health care organizations (Helms et al., 2008). According to Nash (2008), health care organizations typically address security

requirements reactively. Shortcomings and extended requirements in the HIPAA Security Rule relating to business associates, breach notifications, data transmission standards, investigation of complaints, and penalties and enforcement have created liabilities for health care organizations (Brown, 2009b). The findings of this investigation are expected to contribute knowledge that can be applied to improve information security and regulatory compliance in the HIPAA security domain, with a focus on AMCs (Helms et al., 2008; Li & Shaw, 2008).

Third, this study extends prior research on security behavior and security effectiveness by developing a conceptual model of constructs that synthesize multiple theoretical perspectives such as TRA (Ajzen & Fishbein, 1980), TPB (Ajzen, 1985), TAM (Davis, 1989), TAM2 (Venkatesh & Davis, 2000), and UTAUT (Venkatesh et al., 2003). By examining the human, organizational, and technological factors that influence HIPAA security compliance in AMCs, information security researchers and practitioners working in AMCs will be able to understand the areas affecting the current HIPAA security requirements (Keith et al., 2009).

Chapter 3

Methodology

Research Methods Employed

The author chose to conduct a predictive study that used survey methodology to collect data and develop a model of factors that affect HIPAA security compliance in AMCs. Palvia, Leary, Mao, Midha, Pinjani, and Salam (2004) determined that, because a survey methodology has a high degree of external validity, it is appropriate for developing a predictive model.

Specific Procedures Employed

Survey Development

According to Straub (1989), "an instrument valid in content is one that has drawn representative questions from a universal pool" (p. 150). Pinsonneault and Kraemer (1993) maintained that surveys are suitable when independent and dependent variables are clearly defined. Further, Kitchenham and Pfleeger (2002) observed that survey development using existing constructs is common because the validity and reliability tests of existing variables have already been established.

In constructing the survey for this investigation, the author utilized clearly defined constructs and previously validated items to empirically assess the effect of management support, security awareness, security culture, and computer self-efficacy on security behavior and security effectiveness and thus HIPAA security compliance in AMCs. The instrument, which is discussed below, was distributed using the Web. According to Rhodes, Bowie, and Hergenrather (2003), Web-based surveys allow researchers to

quickly communicate to large groups of potential respondents, providing a setting of openness that encourages full participation by respondents and is cost effective. Additionally, Web-based surveys support data collection and eliminate data entry errors (Levy, 2006; Porter & Whitcomb, 2003).

The survey (Appendix A) that was used in this investigation was a multi-item instrument, whose items were answered by a 5-point Likert-type scale. A combination of existing validated scales from the literature were used to develop the survey instrument for this investigation. Leidner and Jarvenpaa (1995) recommended the use of established constructs in lieu of developing new variables. Previously validated survey items that pertain to variables applicable to current research have been used extensively in the literature (Boudreau, Gefen, & Straub, 2001). Therefore, the author developed multi-item measures for each construct by adapting previously validated instruments from prior research. In the completed analysis, the author used MS to represent management support items, SA to represent security awareness items, SC to represent security culture items, CSE to represent computer self-efficacy items, SB to represent security behavior items, and SE to represent security effectiveness items.

Measure of Management Support (MS)

Items for MS in the instrument were adapted from the survey items developed and validated by Knapp et al. (2007) and Lin (2007). To develop a theoretical model, Knapp et al. used a qualitative strategy that closely followed grounded theory. The grounded theory used by Knapp et al. was first introduced by Glaser and Strauss (1967) and further refined as a series of structured steps by Strauss and Corbin (1998). After developing and giving the survey to a sample of information security practitioners, the authors tested the

model using structural equation modeling. They then explored an alternative model in which the mediator variables were represented by a higher order factor. Knapp et al.'s study combined qualitative and quantitative techniques over a six-step methodological process that included: (a) qualitative data collection; (b) qualitative analysis; (c) scale development; (d) instrument refinement; (e) quantitative data collection; and (f) quantitative data analysis. The authors' scale exhibited an acceptable level of internal reliability, with a Cronbach's α reliability of .93 for items related to top management support. Items MS1 to MS6 in the instrument for this study measured the effect of management support on security behavior and security effectiveness and thus HIPAA security compliance in AMCs.

Based on a survey of 172 employees from 50 large organizations in Taiwan, Lin (2007) applied structural equation modeling to investigate a research model for knowledge sharing and firm innovation capability. Lin's four top management support survey items were adapted from studies by Tan and Zhao (2003). The author found that the organizational factor of top management support significantly influenced the knowledge-sharing process. The author performed confirmatory factor analysis, convergent validity, and discriminant validity to determine the reliability of the top management support construct (composite reliability), which was based on the studies of Anderson and Gerbing (1992) and Joreskog and Sorbom (1996). Lin's measurement model for the top management support item demonstrated adequate reliability, convergent validity, and discriminant validity. Items MS7 to MS10 in the instrument for this study measured the effect of management support on security behavior and security effectiveness and thus HIPAA security compliance in AMCs.

Measure of Security Awareness (SA)

Items for SA in the instrument were developed by consolidating and adapting survey items developed and validated by D'Arcy and Hovav (2009), Knapp et al. (2007), and Johnston and Warkentin (2008). D'Arcy and Hovav developed a survey based on Straub's (1990) general deterrence theory, which posits that user awareness of security policies; security education, training, and awareness programs; and computer monitoring directly influence IS misuse intention (i.e., unauthorized access and unauthorized modification). Four items measuring security education, training, and awareness were developed as original scales by D'Arcy and Hovav. The authors' measurement model was assessed by tests of convergent validity, discriminant validity, and reliability. The convergent validity and discriminant validity factor loadings exceeded the recommended values of .70 and .50, respectively, for the four items measuring security education, training, and awareness. In addition, the reliabilities of the constructs were above the recommended .70 threshold specified by Fornell and Larcker (1981). The items SA1 to SA4 in this study's instrument measured the effect of security awareness on security behavior and security effectiveness and thus HIPAA security compliance in AMCs.

Knapp et al. (2007) solicited responses from 220 Certified Information System Security Professionals to the following question: What are the top five information security issues facing organizations today? After several follow-on questions were given to the sample population, the respondent statements were coded into categories and patterns that suggested theoretical relationships. User training was found to be a mediating variable in predicting security effectiveness. Knapp et al. developed five items for the user-training variable, which exhibited high reliability, low cross-loading with

other constructs, and low residual covariance with other items. The user-training construct exhibited an acceptable level of internal reliability, with a Cronbach's α of .93. Items SA5 to SA8 in this study's instrument measured the effect of security awareness on security behavior and security effectiveness and thus HIPAA security compliance in AMCs.

Johnston and Warkentin's (2008) instrument included six items representing HIPAA privacy training. The authors developed the survey items as original scales to test for perceived organizational support. Johnston and Warkentin performed construct validity and reliability tests and found acceptable levels of convergent and discriminant validity for the HIPAA privacy training items. Items SA9 to SA10 in the instrument for this study measured the effect of security awareness on security behavior and security effectiveness and thus HIPAA security compliance in AMCs.

Measure of Security Culture (SC)

Items for SC in the instrument were developed by consolidating and adapting survey items developed and validated by Knapp et al. (2007) and Chan et al. (2005). Based on an analysis of qualitative data, Knapp et al. developed measurement items for SC through a process of extracting words and phrases from the participant responses to build a pool of candidate items. The authors also used the technique of theoretical saturation, drawn from Strauss and Corbin (1998), to determine the appropriate number of items in the SC pool (DeVellis, 2003). Theoretical saturation occurs "when adding items to the pool contributes little marginal value to the scale or seems counterproductive" (Knapp et al., p. 42). An expert panel of 12 Certified Information System Security Professionals further refined the SC measures by determining the construct validity of the items and assessing

the perceived sensitive nature of the security-related questions that were asked. The Cronbach's α for the SC factors was .90. Items SC1 to SC6 in this study's instrument measured the effect of security culture on security behavior and security effectiveness and thus HIPAA security compliance in AMCs.

Chan et al. (2005) developed survey items for SC using a systematic procedure suggested by Churchill (1979). The instrument development process involved specifying the domain for the individuals' perception of the organizational climate construct, delineating what is included and what is excluded, generating sample items from past literature, iteratively refining the instrument through data collection, and assessing the reliability and validity of the data. The authors developed four items representing individuals' perception of organizational climate by adapting survey items used by Schnake (1983) and Neal and Griffin (1997). The items were measured using a 7-point Likert scale anchored from strongly disagree to strongly agree. Testing of the measurement model involved assessing the convergent validity and discriminant validity of the instrument items. The Cronbach's α for the SC factors was .87. Items SC7 to SC10 in the instrument for this study measured the effect of security culture on security behavior and security effectiveness and thus HIPAA security compliance in AMCs.

Measure of Computer Self-Efficacy (CSE)

Items for CSE in the survey were adapted from the survey items developed and validated by Ball and Levy (2008). Based on a study of 56 instructors from a small, private university, the authors, using ordinal logistic regression, assessed the factors that influenced instructors' acceptance of information systems to formulate a predictive model. Ball and Levy developed their CSE survey items from the 10-item CSE

instrument developed by Compeau and Higgins (1995). Compeau and Higgins found the instrument to have a Cronbach's α of .80, thus demonstrating that the CSE items were reliable. The original instrument developed by Compeau and Higgins was based on a 10-point Likert scale, which was subsequently adapted by Chu (2003) into a 5-point Likert scale. The 5-point scale was found to be both reliable and valid for measuring CSE, with a Cronbach's α of .79 in pre-test and .70 in post-test. Items CSE1 to CSE10 in this study's instrument measured the effect of computer self-efficacy on security behavior and security effectiveness and thus HIPAA security compliance in AMCs.

Measure of Security Behavior (SB)

Items for SB in the instrument were developed by consolidating and adapting survey items developed and validated by Chan et al. (2005), Cazier et al. (2007), Hazari et al. (2008), and Johnston and Warkentin (2008). Chan et al. derived five compliant behavior items from self-development, Neal and Griffin (1997) and Hayes, Perander, Smecko, and Trask (1998). The Cronbach's α measure for internal consistency reliability was .90 for the compliant behavior items.

Johnston and Warkentin's (2008) instrument included three variables representing HIPAA compliance behavioral intention. The authors adapted the items from Venkatesh and Davis' (2000) behavioral intention scale for measuring intent for technology adoption. Johnston and Warkentin conducted construct validity tests consistent with those of Loch, Straub, and Kamel (2003), in which a modified multi-trait, multi-method analysis was used to assess factor loadings, convergent validity, and discriminant validity. Based on their analysis, Johnston and Warkentin determined that there were acceptable levels of factor loadings, convergent validity and discriminant validity for the

HIPAA compliance behavioral intention items. Item SB6 in the instrument was adapted from Johnston and Warkentin's measure.

Cazier et al.'s instrument included three variables representing behavioral intention. The Cronbach's α measuring confidentiality for SB7 through SB9 in Cazier et al.'s instrument was .79. Items SB7 through SB9 in the study's instrument were adapted from Cazier et al.'s measure. Hazari et al.'s instrument included three variables representing information security behavioral intention. Although the Cronbach's α of the authors' overall scale was .88, the Cronbach's α for the information security behavioral intention items was only .66. Item SB10 in the instrument was adapted from Hazari et al.'s measure.

Measure of Security Effectiveness (SE)

Items for SE in the study's instrument were developed by consolidating and adapting survey items developed and validated by Knapp et al. (2007) and Chang and Lin (2007). Knapp et al.'s instrument included five items for SE. In their instrument, the Cronbach's α for internal consistency reliability was .91. Items SE1 through SE5 in this study's instrument were adapted from the measures developed by Knapp et al. Chang and Lin's instrument included four variables representing information security management effectiveness, including five items for confidentiality, five items for integrity, three items for availability, and six items for accountability. The Cronbach's α for confidentiality for SE6 through SE8 in Chang and Lin's instrument was .88; for integrity for SE9 and SE11, .717; and for accountability for SE1, .87. Items SE6 through SE12 in the instrument were adapted from Chang and Lin's measures.

Population and Sample

The target population of this study was health care professionals who are associated with the AAMC (AAMC, 2009a). The AAMC represents the 131 accredited U.S. medical schools and 17 accredited Canadian medical schools, approximately 400 major teaching hospitals and health systems, and nearly 90 academic and professional societies (AAMC, 2009a). Nearly 125,000 faculty members, 75,000 medical students, and 106,000 resident physicians are represented by the aforementioned institutions and organizations comprising the AAMC (AAMC, 2009a).

The target sample of this study was health care professionals who are members of the Group on Information Resources (GIR) within the AAMC (AAMC, 2009b). The GIR provides:

> a forum for individuals in relevant roles of leadership and responsibility to promote excellence in the advancement of information resources in academic medicine, including medical education, clinical care, medical and health sciences research, health science libraries, public health, and institutional planning (M. Passiment, personal communication, August 14, 2009, para. 3).

The GIR membership consists of approximately 590 IT professionals (AAMC, 2009b). Chief information officers and vice presidents comprise 26% of the group; IT directors, 18%; administrators, 17%; library technologists, 17%; educational technologists, 6%; clinicians, 5%; informatics professionals, 4%; faculty and educators, 4%; and researchers, 3% (M. Passiment, personal communication, para. 5). The survey was distributed to the membership list of the GIR via e-mail. This e-mail also stated the purpose of the investigation and requested their participation in completing the survey.

Survey Implementation to Collect Data

Permission was requested from the AAMC's Director of Information Resources Outreach to send the Web-based survey information to the GIR members. After obtaining permission from the AAMC Director Information Resources Outreach, approval from the Nova Southeastern University (NSU) Institutional Review Board (IRB) was requested. Prior to requesting permission from the AAMC Director Information Resources Outreach and the NSU IRB, permission was obtained from the author's dissertation committee. With the permission of the dissertation committee, the AAMC Director Information Resources Outreach and the NSU IRB, an e-mail with the Web-based survey and instructions, along with an explanation of the purpose and relevance of the study, was sent to the survey participants by the Director of Information Resources on behalf of the author and the AAMC.

Participation in the survey by the AMC GIR members was anonymous. To increase the response rate, the AAMC Director of Information Resource Outreach sent out a second e-mail after two weeks to the AAMC GIR members as a reminder to participate in the survey. As indicated by Kaplowitz, Hadlock, and Levine (2004), response rates of Web-based surveys were reported to improve with the use of reminder notifications. When the Web-based survey were completed, the data from the survey was imported into Statistical Package for Social Science (SPSS) Statistics 18.0 for statistical data analysis (SPSS, n.d.).

Pre-analysis Data Screening

The author included a pre-analysis data screening procedure to ensure the validity of the survey responses. According to Levy (2006), pre-analysis data screening aids in

detecting irregularities or problems with the data collected. Pre-analysis data screening is required before data analysis to ensure that the conclusions are based on valid data (Mertler & Vannatta, 2001). According to Levy, there are four main reasons for pre-analysis data screening.

First, pre-analysis data screening ensures the accuracy of the data collected. According to Levy (2006), "if the data collected is not accurate, the analysis will not be valid either" (p. 150). To eliminate data entry or typing errors, the data will be imported directly from the Web-based survey to a spreadsheet, and then to statistical software formats.

Second, pre-analysis data screening addresses the issue of response-set. Kerlinger and Lee (2000) suggested that "response-set can be considered a mild threat to valid measures" (p. 713). Kerlinger and Lee defined response-set as a set of responses for which respondents submit the same score for all items. To address the issue of response-set, the data collected from the Web-based survey will be reviewed for elimination prior to the final analyses.

Third, pre-analysis data screening deals with missing data. According to Mertler and Vannatta (2001), "missing data can significantly affect the validity of the data collected and the results drawn from it" (p. 25). To eliminate missing data, the Web-based survey will be configured to require that all survey items will be answered.

Finally, pre-analysis data screening addresses outliers or extreme cases. Levy (2006) stated that identifying data outliers "is required as it is inadequate to draw conclusions from data that is skewed by a number of extreme cases" (p. 152). Mertler and Vannetta (2001) noted that "an outlier can cause a result to be insignificant when, without the outlier, it would have been significant" (p. 27). To address the issue of outliers or extreme

cases, Mahalanobis Distance analysis was performed on the survey responses prior to data analyses. Mahalanobis Distance analysis is an often used technique for determining the similarity of an unknown sample set to a known one (Sun et al., 2000). According to Hair, Anderson, Tatham, and Black (1984), Mahalanobis Distance analysis is useful in identifying extreme cases and whether data should be kept or discarded during data analysis.

Validity and Reliability

The validity and reliability of the instrument were tested in the context of the investigation. According to Leedy and Ormrod (2005), "the validity and reliability of your measurement instruments influences the extent to which you can learn something about the phenomenon you are studying . . . and the extent to which you can draw meaningful conclusions from your data" (p. 31). Reliability refers to "the consistency with which a measuring instrument yields a certain result when the entity being measured has not changed" (p. 31). As indicated by Carmines and Zeller (1991), reliability can be established in four ways: equivalency reliability, stability reliability, inter-rater reliability, and internal consistency. Internal consistency "focuses on the level of agreement among the various parts of the instrument or process in assessing the characteristic being measured" (Ellis & Levy, 2009, p. 334). In this study, the internal consistency of each variable's survey items was measured through correlations using the Cronbach's α coefficient.

Validity is defined as a researcher's ability to "draw meaningful and justifiable inferences from scores about a sample or population" (Creswell, 2005, p. 600). The validity of an instrument refers to "the extent to which the instrument measures what it is

supposed to measure" (Leedy & Ormrod, 2005, p. 31). Types of validity include internal, face, criterion-related, construct, content, statistical conclusion, and external validities (Ellis & Levy, 2009). This investigation examined three validity measures of the instrument: content validity, construct validity, and external validity.

In survey-based research, content validity is defined as "the degree to which items in an instrument reflect the content universe to which the instrument will be generalized" (Boudreau et al., 2001, p. 5). Construct validity "is in essence an operational issue. It asks whether the measures chosen are true constructs describing the event or merely artifacts of the methodology itself" (Straub, 1989, p. 150). External validity refers to the "extent to which its results apply to situations beyond the study itself . . . the extent to which the conclusions drawn can be generalized to other contexts" (Leedy & Ormrod, 2005, p. 105). King and He (2005) stated that external validity addresses the "generalizability of sample results to the population of interest, across different measures, persons, settings, or times. External validity is important to demonstrate that research results are applicable in natural settings, as contrasted with classroom, laboratory, or survey-response settings" (p. 882).

Data Analysis

After the pre-analysis data screening procedure, the tests for reliability and validity, and the final screening of the dataset, further statistical analyses were performed. The means and standard deviations for the multiple item scores that comprised MS, SA, SC, CSE, SE, and SB were calculated to create six composite variables. Kolmogorov-Smirnov *Z* statistics were used to test the null hypothesis that the variables were normally distributed.

The effects of the independent variables on the dependent variables were investigated through multiple linear regression (MLR). MLR analysis is defined as "a statistical technique to predict the variance in the dependent variable by regressing the independent variables against it" (Sekaran, 2003, p. 420). Sprinthall (1977) stated that MLR analysis is useful for predicting the dependent variable based on multiple independent variables. According to Chen and Hughes (2004), MLR uses independent variables to predict the probability of the dependent variable using a linear approach. MLR analysis assumes that the residuals (the differences between the predicted and observed values) are normally distributed. This normal distribution was validated by visually inspecting a frequency distribution histogram and tested through Kolmogorov-Smirnov *Z* statistics.

MLR analysis also assumes that the relationship between the independent and dependent variables is linear. The assumption that the residuals were randomly and relatively evenly scattered on either side of their mean (zero) value with respect to the predicted values, reflecting homogeneity of variance of the dependent variable, was checked visually using a plot of the residuals versus the predicted values. Additionally, statistical analysis for the presence of linearity between the MS, SA, SC, CSE, SB, and SE variables was performed using Pearson's correlation coefficients.

Pearson correlation analysis also was used to assess the possibility of excessive collinearity (Tabachnik & Fidell, 2007). A second method to test for excessive collinearity involved calculating the variance inflation factor (*VIF*) statistic (O'Brien, 2007). Collinearity is a significant problem when the research methodology is designed to predict the effect of the independent variables on the dependent variable. When excessive collinearity is present, the standard errors are inflated, influencing the signs and

the magnitudes of the regression coefficients, which results in the inability to accurately assess the relative importance of each of the predicting variables (Tabachnik & Fidell).

According to Chen and Hughes (2004), ordinal linear regression (OLR) uses multiple independent variables to predict the probability of the dependent variable using a non-linear approach. As indicated by Hoffman (2004), OLR analysis does not assume linear relationships or necessitate that the data be normally distributed. OLR is therefore considered appropriate for measuring the effect of the independent variables on the dependent variable (Chen & Hughes). However, to artificially create non-continuous mutually exclusive categories, OLR analysis requires rounding the mean values of the independent and dependent variables down to integers. The literature, however, is inconclusive as to whether this technique is statistically correct (Bowker & Randerson, 2010; Kim, 1975). In this study, the independent and dependent variables were continuous and quantitative and measured at the scale/interval level. In addition, the variables were linear and normally distributed. Therefore, MLR analysis was justified.

MLR Analysis to Predict Security Behavior

The general multiple regression equation used in this study to predict the effect of the four independent variables on the first dependent variable was defined as:

$$Y_1 = \beta_0 + \beta_1 X_1 + \beta_2 X_2 + \beta_3 X_3 + \beta_4 X_4 + e$$

The MLR model used in this investigation to predict the effect of MS, SA, SC, and CSE on SB was:

$$SB = \beta_0 + \beta_{MS}*MS + \beta_{SA}*SA + \beta_{SC}*SC + \beta_{CSE}*CSE + e$$

where SB is the predicted value of the dependent variable Security Behavior, β_0 is the intercept or constant of the equation (the theoretical predicted value of the dependent

variable when all the independent variables are zero), β_{MS} is the strength of MS, MS is the average of all MS survey items, β_{SA} is the strength of SA, SA is the average of all SA survey items, β_{SC} is the strength of SC, SC is the average of all SC survey items, β_{CSE} is the strength of CSE, CSE is the average of all CSE survey items, and e is the random error.

MLR Analysis to Predict Security Effectiveness

The general multiple regression equation used in this study to predict the effect of the four independent variables on the second dependent variable was defined as:

$$Y_2 = \beta_0 + \beta_1 X_1 + \beta_2 X_2 + \beta_3 X_3 + \beta_4 X_4 + e$$

The MLR model used in this investigation to predict the effect of MS, SA, SC, and CSE on SE was:

$$SE = \beta_0 + \beta_{MS}*MS + \beta_{SA}*SA + \beta_{SC}*SC + \beta_{CSE}*CSE + e$$

where SE is the predicted value of the dependent variable Security Effectiveness, β_0 is the intercept or constant of the equation (the theoretical predicted value of the dependent variable when all the independent variables are zero), β_{MS} is the strength of MS, MS is the average of all MS survey items, β_{SA} is the strength of SA, SA is the average of all SA survey items, β_{SC} is the strength of SC, SC is the average of all SC survey items, β_{CSE} is the strength of CSE, CSE is the average of all CSE survey items, and e is the random error.

The strength or standardized partial regression coefficient of each independent variable measured the change in the dependent variable for each unit change in the independent variable (Sprinthall, 1977). According to Tabachnik and Fidell (2007), the higher the magnitude of the standardized partial coefficient, the more important the

independent variable is as a predictor of the dependent variable, assuming that its magnitude is not biased by collinearity. Standardized coefficients or β weights are more useful than are unstandardized coefficients because they enable the researcher to interpret the relative importance of each independent variable, especially if each is measured using different scales or units (Tabachnik & Fidell).

Power Analysis

The author performed a post-hoc power analysis to validate that the sample size was adequate to permit the rejection of the null hypothesis of MLR. In cases for which the adjusted R^2 does not explain a substantial portion of the variance in the dependent variable, a power analysis is appropriate (Cohen, 1992). A power analysis was completed for each dependent variable in the study.

Formats for Presenting Results

The results of the data analyses were presented in various tables and figures in the results section of this dissertation. Conclusions were derived from the data reported in the tables and figures and summarized accordingly. The MLR and correlation analyses that were used to investigate the relationship between the independent variables and the dependent variables also were discussed.

Resources Used

To conduct the survey, the author worked with the following:

1. NSU dissertation advisor and committee
2. NSU IRB advisor

3. AAMC GIR Director of Information Resources Outreach

4. AAMC GIR members

5. AAMC IRB Board representative

The Web-based survey was conducted using the electronic survey software, SurveyMonkey® (n.d.). After the survey was complete, data from the survey were downloaded from SurveyMonkey®, underwent pre-analysis, and were analyzed with the appropriate statistical techniques using SPSS Version 18.0 (SPSS, n.d.). Throughout this investigation, the author used NSU's digital library resources (NSU Libraries, n.d.).

Summary

In this investigation, the author developed a 61-item Web-based survey, which used Likert-scaled multiple items to determine the factors affecting HIPAA security compliance in AMCs. This Web-based survey was developed using a combination of existing and validated scales for the independent variables, MS, SC, SC, and CSE, and the dependent variables, SE and SB. The target population was health care professionals associated with the AAMC. The sample for this empirical study was 590 health care information technology professionals who were members of the GIR within the AAMC.

The author included a pre-analysis data screening procedure to ensure the validity of the survey responses. The validity and reliability of the instrument were tested in the context of the investigation. After the dataset underwent final screening, further statistical analyses were performed. These included testing for the mean and standard deviation as well as using Kolmogorov-Smirnov *Z* statistics and frequency distribution histograms to test the null hypotheses that the variables were normally distributed. Pearson correlation

analysis was computed to validate that the relationship between the independent and dependent variables was linear. Additionally, Pearson correlation analysis and the calculation of the *VIF* statistic were used to test for the presence of excessive collinearity.

MLR analysis was used to derive and validate the theoretical models to predict the effect of the four independent variables of management support, security awareness, security culture, and computer self-efficacy on security behavior and security effectiveness and thus HIPAA security compliance in AMCs. A post-hoc power analysis was performed to validate that the sample size was adequate to permit the rejection of the null hypothesis of MLR. The outcomes of this study are expected to enhance the understanding of HIPAA security compliance in AMCs. The results of this research also are expected to provide guidance to individuals and organizations involved with HIPAA security-compliance initiatives in health care.

Chapter 4

Results

Overview

This chapter presents the results of the statistical analyses used in the investigation. The effect of four independent variables, management support, security awareness, security culture, and computer self-efficacy, on the two dependent variables, secure behavior and security effectiveness, and thus HIPAA security compliance in AMCs, was explored. First, the data collection procedures are presented, followed by the results of the pre-analysis data screening. Then the validity and reliability findings are reviewed, followed by the results of the multiple regression analysis. The chapter concludes with a summary. To enhance understanding, the chapter sections are organized similarly to those of Chapter 3.

Data Collection and Analysis

Data Collection

The online survey instrument (Appendix A) was designed and delivered in a Web-based format. A Web-based survey instrument was selected as the delivery method because an electronic format allows for direct respondent input. Because no manual input was required, data entry errors were minimized. On April 6, 2010, the AAMC Director of Information Resources e-mailed the 590-member AAMC GIR group a link to the Web-based survey. A response rate of at least 25% was anticipated. A total of 76 AAMC GIR members completed the survey, yielding a response rate of approximately 12.9%. According to Shevade and Keerthi (2003) and Komarek and Moore (2004),

approximately 100 respondents are generally required to achieve statistically significant results in regression analysis. However, a post-hoc power analysis validated that responses from 76 GIR members adequately ensured that the sample was representative of the population and therefore ensured the generalizability of the study's findings (Cohen, 1992).

Pre-Analysis Data Screening

To ensure the validity of the survey responses, the author included pre-analysis data screening. Pre-analysis data screening was important for four reasons. First, pre-analysis data screening ensures the accuracy of the data collected. In the study, data accuracy was not an issue because the Web-based survey software used to collect the data did not require free text responses. In addition, the data were downloaded directly for analyses from the Web-based software. Second, pre-analysis data screening addresses the issue of response-set. In the study, response-set was not an issue because no survey submissions included the same score for 100% of the survey items. Third, pre-analysis data screening concerns missing data. Missing data were not a factor in the study because the respondents were required to answer all of the survey items to complete the survey.

Finally, pre-analysis data screening addresses multivariate outliers or cases with patterns of scores that are extreme or abnormal. Because the intention was to analyze the responses collectively using multiple regression analysis, screening for multivariate outliers was necessary. Mahalanobis Distance (D^2) values were calculated for each case using the technique described by Hisham (2008). D^2 measures the distance of a case from the centroid (multidimensional mean) of a distribution, taking into account the covariance (multidimensional variance) of the distribution. As indicated by Hisham, Mahalanobis D^2

values closely follow a *chi*-square distribution with *n* degrees of freedom, where *n* = the number of independent variables, when the variables used to compute the mean vector and covariance matrix are assumed to be normally distributed. Because *n* = 4 (i.e., MS, SA, SC, and CSE) in the investigation, the SPSS syntax used to calculate the *p* value from the *chi*-square distribution with *df* = 4 degrees of freedom would be less than the computed value of D^2, which was 1 – CDF.CHSQ (D^2, 4). All of the *p* values for the computed Mahalanobis D^2 values exceeded .001. The smallest *p* value was .008, providing evidence that the variables included no multivariate outliers at the .001 level of significance. It was assumed, therefore, that MLR analysis would not be compromised by the presence of outliers, and thus all 76 cased could be included. The Mahalanobis Distance analysis results are presented in Figure 7.

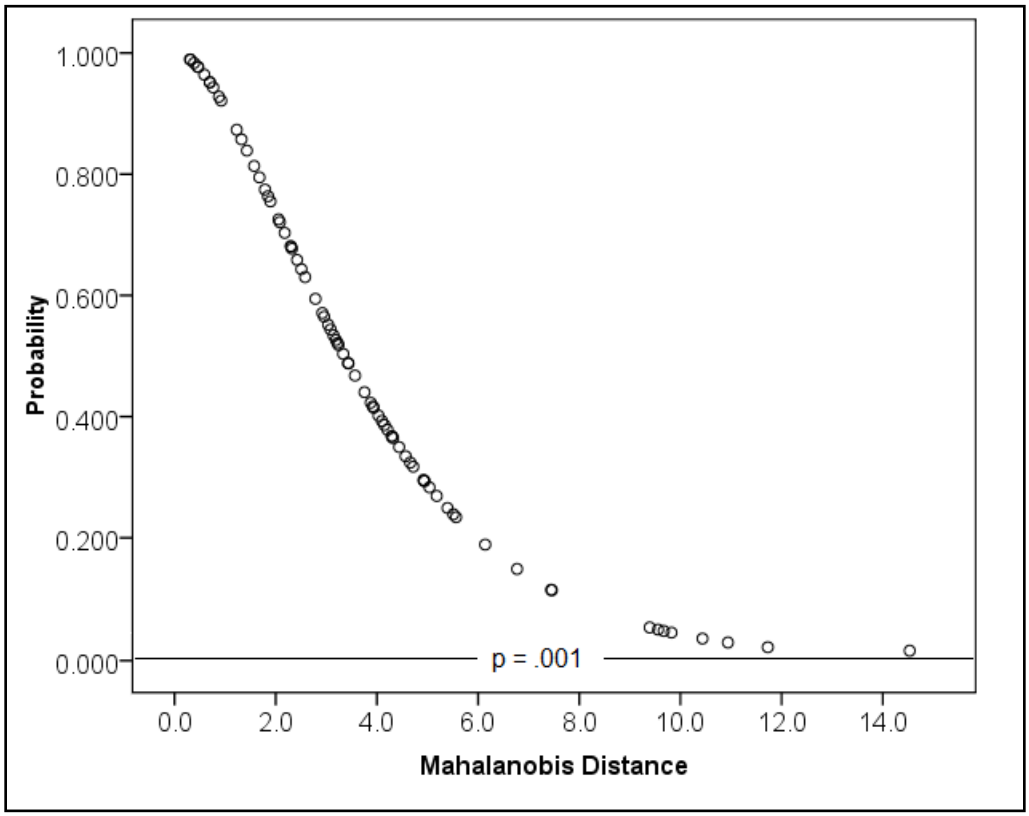

Figure 7. Mahalanobis Distance analysis.

Validity and Reliability

The author examined three validity measures of the instrument: content validity, construct validity, and external validity. According to Sun and Zhang (2006), validity is an important concern in survey-item development. Further, survey items should be representative of all aspects of the variables being examined (Lewis, Templeton, & Byrd, 2005). The author achieved content validity, construct validity, and external validity of the 61 survey items by basing the survey items on previously validated scales drawn from the literature.

Cronbach's α reliability tests were computed to determine the internal consistency for the survey items MS, SA, SC, CSE, SE, and SB. All items were reviewed to ensure that all scales were keyed in the same direction (Levy, 2006). To avoid negative items in the survey, items SB2, SB3, SB4, and SB5 were inversely scored, and the reliability tests were performed again. The final analysis resulted in high reliability scores for each variable, with Cronbach's α well above the desired minimum of .70 (Sprinthall, 1997). MS and SA had the highest internal consistency reliability (α = .943 and .941), whereas SB had the lowest reliability (α = .807). The reliability analysis results for the survey items are presented in Table 8.

Table 8. Reliability Analysis Results

Variable	Number of Cases	Number of Items	Cronbach's *a*
MS	76	10	.943
SA	76	10	.941
SC	76	10	.920
CSE	76	10	.881
SE	76	11	.930
SB	76	10	.807

Data Analysis

Following the pre-analysis data screening, as well as validity and reliability tests, the mean values for the multiple item scores that comprised MS, SA, SC, CSE, SE, and SB were calculated to create six composite variables. The mean values of the independent and dependent variables were between 3.2 and 4.2, indicating a general tendency for the numerically-coded responses to represent a value somewhere between neither disagreeing nor agreeing with the items (score = 3) and agreeing with the items (score = 4). The standard deviations of all of the variables ranged from .49 to .71, indicating a relatively wide variability in the responses. Kolmogorov-Smirnov *Z* statistics were used to test the null hypotheses that the variables were normally distributed. Based on the results, which were non-significant, the null hypotheses were accepted. The parametric descriptive statistics for each composite variable and tests for normality are presented in Table 9.

Table 9. Descriptive Statistics and Tests for Normality

	MS	**SA**	**SC**	**CSE**	**SE**	**SB**
Number of cases	76	76	76	76	76	76
Mean	3.900	4.000	3.800	3.200	3.900	4.200
Standard deviation	.710	.680	.630	.690	.650	.490
Kolmogorov-Smirnov *Z*	.794	.850	.682	1.56	.986	1.254
p	.554	.465	.741	.056	.285	.086

The approximately bell-shaped frequency distribution histograms also provided visual evidence to suggest that the variables MS, SA, SC, CSE, SE, and SB were normally distributed. As a result, parametric statistics assuming normality were justified. The frequency distributions for each variable are presented in Figure 8.

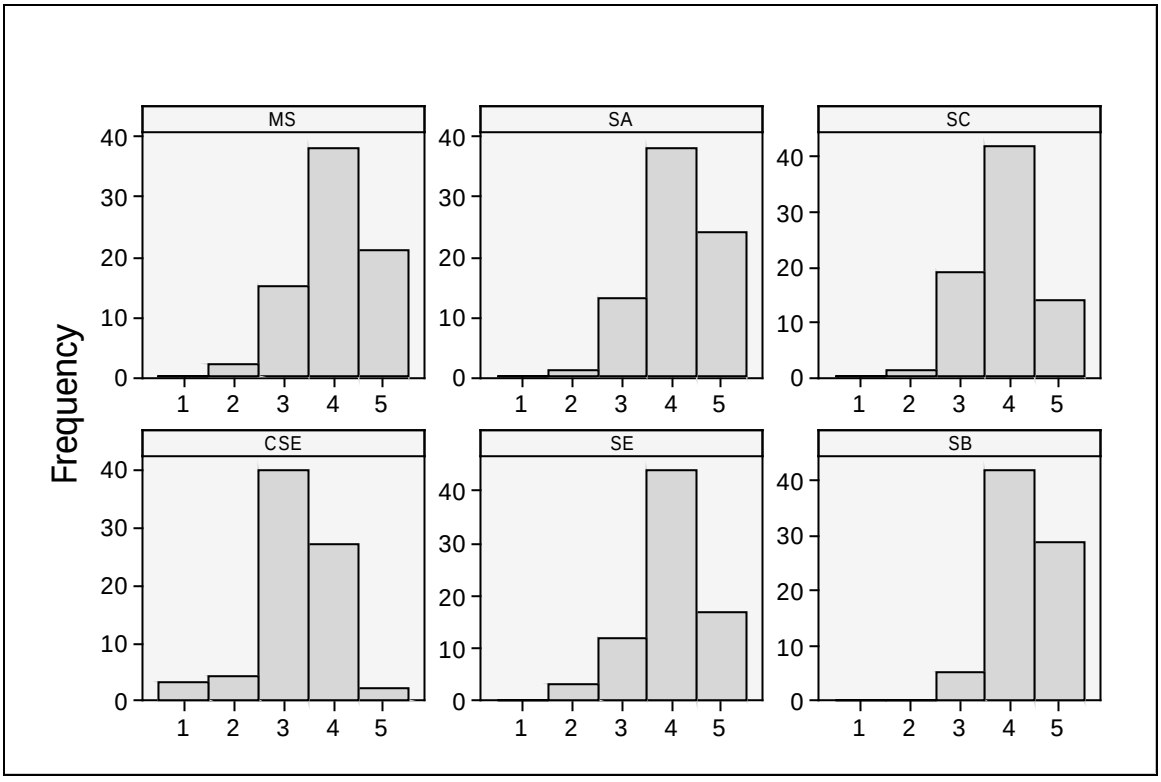

Figure 8. Frequency distributions of the variables.

The author initially reviewed two regression methods, MLR and OLR analyses, to measure the effect of the independent variables, MS, SA, SC, and CSE, on the dependent variables, SE and SB. According to Chen and Hughes (2004) and Tabachnik and Fidel (2007), MLR analysis is used predict the values of normally distributed dependent variables measured at the scale/interval level. OLR analysis, in comparison, is used to predict the values of dependent variables that are classified into ordinal categories, measured using integers (Hoffman, 2004). OLR analysis does not assume linear relationships or necessitate that the data be normally distributed. In this investigation, the dependent variables, SE and SB, were not measured as ordinal categories but were computed as mean values, measured at the scale/interval level. As a result, for the purposes of this study, MLR analysis was considered to be more appropriate than was OLR analysis.

MLR analysis assumes that the residuals (the differences between the predicted and observed values) are normally distributed. The author visually checked that the residuals were normally distributed by using a frequency distribution histogram (Figure 8). In addition, Kolmogorov-Smirnov *Z* statistics (Table 9) indicated that the variables were normally distributed. The author confirmed that the residuals were randomly and relatively evenly scattered on either side of their mean (zero) value with respect to the predicted values, reflecting homogeneity of variance of the dependent variable, by visually using a plot of the residuals versus the predicted values (Figure 9). The matrix of scatter plots between the variables is presented in Figure 9.

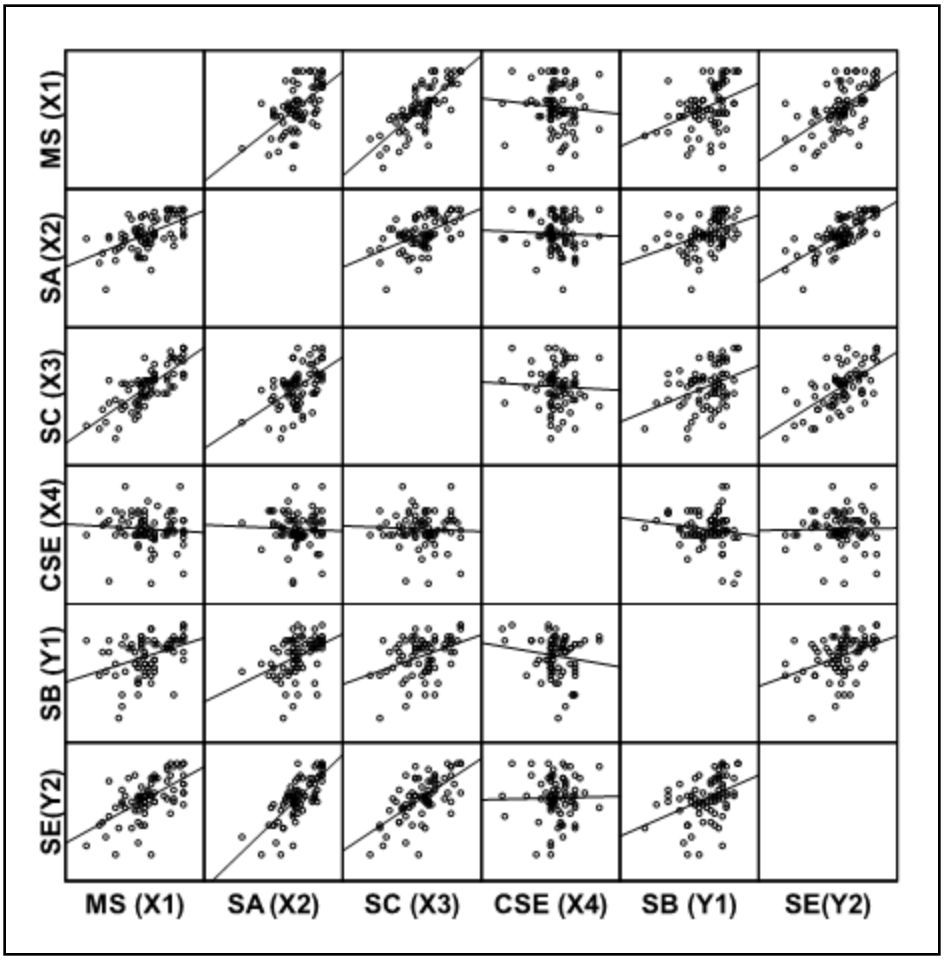

Figure 9. Matrix of scatter plots between the variables.

MLR analysis also assumes that the relationship between the independent and dependent variables is linear. Linearity implies that the average change in the dependent variable associated with a unit change in the independent variable is constant. In addition to visually inspecting the matrix of scatter plots to test for the assumption of linearity (Figure 9), statistical analysis for the presence of linearity was tested using Pearson's correlation coefficients (Table 10). The matrix of Pearson's correlation coefficients between the variables is presented in Table 10.

Table 10. Matrix of Pearson's Correlation Coefficients between the Variables

	MS (X_1)	**SA (X_2)**	**SC (X_3)**	**CSE (X_4)**	**SB (Y_1)**
SA (X_2)	.567**				
SC (X_3)	.776**	.529**			
CSE (X_4)	-.083	-.044	-.049		
SB (Y_1)	.382**	.419**	.381**	-.152	
SE (Y_2)	.600**	.753**	.647**	.020	.401**

** $p < .01$

The linear relationships between the MS, SA, SC, SB, and SE variables were confirmed by the values of Pearson's correlation coefficients between .381 and .776 significant at $p < .01$ and observed in the scatter plots (Figure 9). The CSE variable, however, was not linearly related to the other variables. Further, the Pearson correlation analysis results demonstrated that the independent variables MS, SA, and SC were collinear. According to Tabachnik and Fidell (2007), collinearity is the inter-correlation between the predicting variables in an MLR model. When the inter-correlation is excessive, the standard errors are inflated, influencing the signs and the magnitudes of the regression coefficients, resulting in the inability to accurately assess the relative importance of each of the predicting variables (Tabachnik & Fidell). Collinearity is a significant problem when the research methodology is designed to predict the effect of the independent variables on the dependent variable. As indicated by O'Brien (2007), the researcher must decide how rigorous he or she wants to be when assessing the possibility of excessive collinearity.

According to Tabachnik and Fidell (2007), a Pearson correlation analysis assesses the possibility of excessive collinearity. The authors reported that, when a correlation coefficient matrix includes correlations of approximately 0.7 or higher, excessive collinearity may exist. In this investigation, the correlation coefficient of 0.776 between the MS and SC independent variables was an indication of excessive collinearity that could potentially compromise MLR analysis results. A second method to evaluate the effect of excessive collinearity is calculating the *VIF* statistic (O'Brien, 2007). Although *VIF* values are always greater than or equal to 1, the literature does not indicate how large *VIF* values should be to influence a dependent variable. According to O'Brien, some researchers report that *VIF* values over 2.5 indicate excessive collinearity, while other researchers apply more lenient *VIF* cut-offs of 4.0 or higher for excessive collinearity. To ensure that excessive collinearity did not compromise the results, the *VIF* cut-off value used in this investigation was 2.5 (Alison, 1998).

The MLR model used in this investigation was:

$$SB = \beta_0 + \beta_{MS}*MS + \beta_{SA}*SA + \beta_{SC}*SC + \beta_{CSE}*CSE + e$$

$$SE = \beta_0 + \beta_{MS}*MS + \beta_{SA}*SA + \beta_{SC}*SC + \beta_{CSE}*CSE + e$$

where β_0 represented the intercept or the theoretical predicted value of the dependent variable when all the independent variables were zero; and $\beta_{MS,}$ $\beta_{SA,}$ $\beta_{SC,}$ and β_{CSE} represented the standardized partial regression coefficients for the independent variables. The null hypotheses in the investigation were that the intercept and partial regression coefficients were zero and that the adjusted R^2 value did not explain a substantial proportion of the variance in the dependent variables. The adjusted R^2 was used to account for the number of independent variables in the model. The null hypotheses were

tested using *t* statistics for the regression coefficients and ANOVA *F* statistics for the R^2 value (Tabachnik & Fidell, 2007).

Results of MLR Analysis to Predict Security Behavior

The MLR model calculated by SPSS to predict SB using standardized coefficients was:

SB = 2.960 + .091*MS + .279*SA + .157*SC - .124*CSE + 0

The adjusted R^2 = .187 indicated that the model predicted a significant proportion of the variance in SB. The value of $p < .05$ for the *t* statistics indicated that the intercept was not zero and that SB increased significantly with respect to SA. The value of $p > .05$ for the *t* statistics indicated that the MLR coefficients for MS, SC, and CSE were not significantly different from zero, thus indicating they were not important predictors of SB. However, this model violated the statistical assumptions of MLR with respect to collinearity. The *VIF* statistics > 2.5 indicated that MS (2.763) and SC (2.592) were collinear, therefore demonstrating that the regression coefficients and *p* values may be biased. Due to the presence of collinearity, the author concluded that the MLR model defined in Tables 11 through 13 was inadequate to properly interpret the relationships between the independent and dependent variables. The adjusted R^2 and standard error results to predict SB are presented in Table 11; the MLR coefficients to predict SB are presented in Table 12; and the collinearity statistics to predict SB are presented in Table 13. Overall, Tables 11 through 13 summarize the MLR analysis results to predict SB.

Table 11. Adjusted R Square and Standard Error to Predict SB

Adjusted R^2	**Standard Error of the Estimate**
.187	.446

Table 12. MLR Coefficients to Predict SB

	β	***t***	***p***
Intercept	2.960	6.696	.000***
MS	.091	.528	.599
SA	.279	2.171	.033*
SC	.157	.937	.352
CSE	-.124	-1.191	.238

* $p < .05$, *** $p < .001$

Table 13. Collinearity Statistics to Predict SB

Variable	***VIF***
MS	2.763[a]
SA	1.519
SC	2.592[a]
CSE	1.008

Note. a indicates excessive collinearity.

To correct the MLR model for the influence of excessive collinearity, a new composite variable, MS x SC, was created. The MLR model to predict the dependent variable, SB, including MS x SC, using standardized coefficients was:

SB = 3.311 + .265*SA - .122*CSE + .255*MS x SC + 0

The adjusted R^2 = .204 indicated that this model predicted a higher proportion of the variance in SB, and the standard error was lower. The value of $p < .05$ for the *t* statistics

indicated that the intercept was not zero and that SB increased significantly with respect to both SA and MS x SC. The values of $p > .05$ for the *t* statistic indicated that the regression coefficients for CSE were not significantly different from zero, thus indicating that CSE was not a significant predictor of SB. Additionally, performing MLR analysis for the model with CSE removed produced the adjusted $R^2 = .200$, providing further evidence that CSE did not contribute to the explanation of the variance in the dependent variable.

The revised MLR model to predict the dependent variable, SB, including MS x SC, did not violate the statistical assumptions of MLR with respect to excessive collinearity. The *VIF* statistics < 2.5 indicated that the independent variables, MS (1.516), SA (1.511), and CSE (1.005), were not collinear, thereby demonstrating that the MLR statistics were not biased. The adjusted R^2 and standard error results to predict SB, including MS x SC, are presented in Table 14; the MLR coefficients to predict SB, including MS x SC, are presented in Table 15; and the collinearity statistics to predict SB, including MS x SC, are presented in Table 16. Overall, Tables 14 through 16 summarize the MLR analysis results to predict SB, including MS x SC.

Table 14. Adjusted R^2 and Standard Error to Predict SB, Including MS x SC

Adjusted R^2	**Standard Error of the Estimate**
.204	.441

Table 15. MLR Coefficients to Predict SB, Including MS x SC

	β	***t***	***p***
Intercept	3.311	8.344	.000***
SA	.265	2.096	.040*
MS x SC	.255	2.010	.048*
CSE	-.122	-1.178	.243

* $p < .05$, *** $p < .001$

Table 16. Collinearity Statistics to Predict SB, Including MS x SC

Variable	***VIF***
SA	1.511
MS x SC	1.516
CSE	1.005

The approximately bell-shaped frequency distribution histogram visually indicates that the residuals for the MLR model to predict SB including MS x SC were normally distributed. Residual normality was also confirmed by the recalculated Kolmogorov-Smirnov $Z = .818$, $p = .515$. The residuals were not evenly distributed around their mean (zero) value, reflecting heteroskedacity or differing variances. However, the residuals displayed a definitive wedge-shaped pattern, indicating that the variances evenly decreased with respect to an increase in the predicted values of SB. The revised MLR model was considered to be a good fit for the two independent variables SA and CSE, the

composite independent variable, MS x SC, and the dependent variable SB. The author concluded that, by comparing the magnitudes of the revised MLR coefficients, SA (β = .265) was a more significant predictor of SB than was MS x SC (β = .255). The distribution of residuals for the MLR model to predict SB, including MS x SC, is presented in Figure 10.

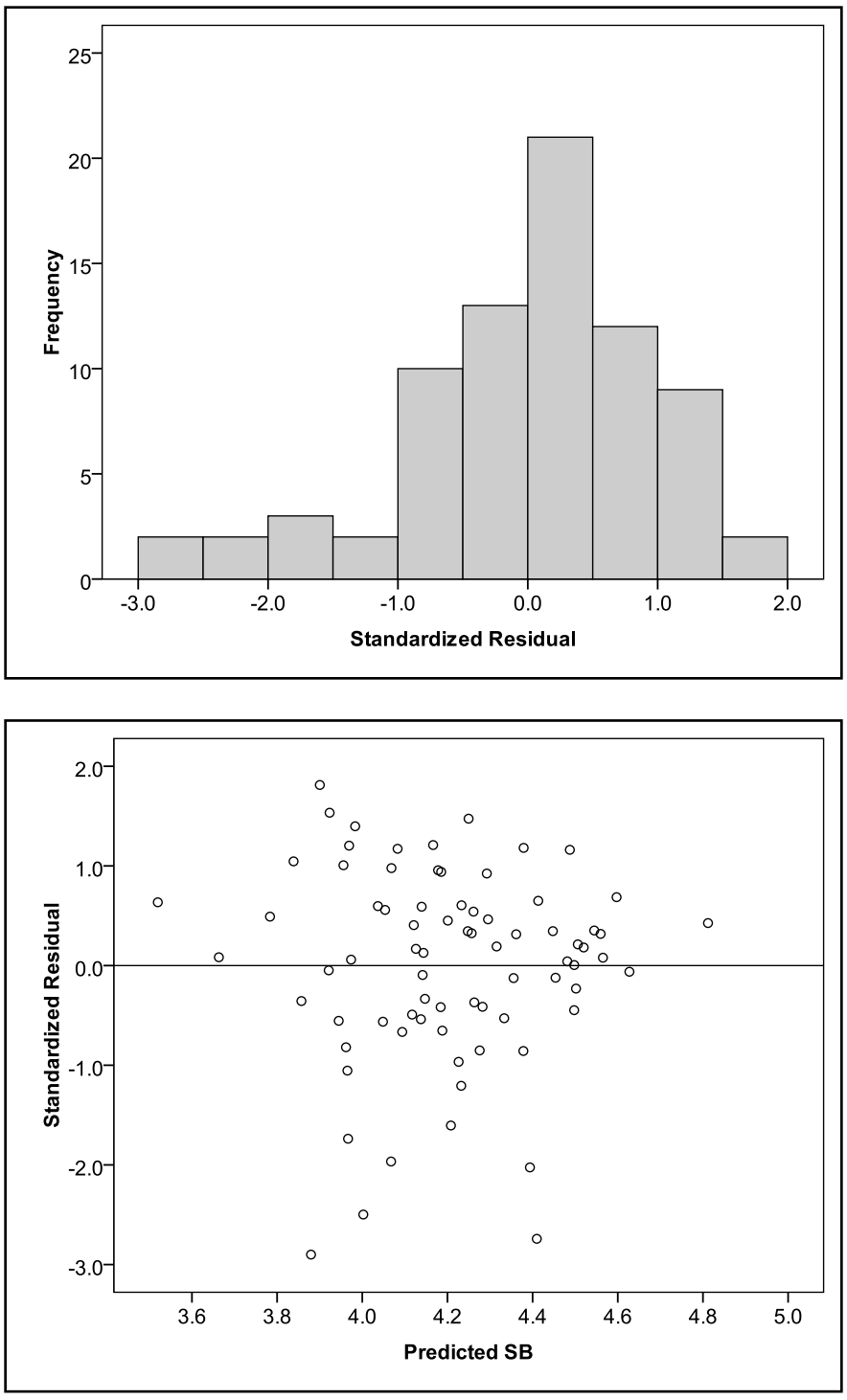

Figure 10. Distribution of residuals for the MLR model to predict SB, including MS x SC.

Results of MLR Analysis to Predict Security Effectiveness

The MLR model calculated by SPSS to predict SE using standardized coefficients was:

SE = .158 + .029*MS + .565*SA + .329*SC + .064*CSE + 0

The adjusted R^2 = .657 indicated that the model predicted a significant proportion of the variance in SE. The adjusted R^2 for the prediction of SE (65.7%) was significantly higher than the adjusted R^2 for SB. In addition, the standard error for the prediction of SE was lower than the standard error for the prediction of SB. The value of $p < .05$ for the *t* statistics indicated that SE increased significantly with respect to both SA and SC. The value of $p > .05$ for the *t* statistics indicated the intercept was not zero and that the MLR coefficients for MS and CSE were not significantly different from zero, thus indicating they were not important predictors of SE. However, this model violated the statistical assumptions of MLR with respect to collinearity. The *VIF* statistics > 2.5 indicated that MS (2.763) and SC (2.592), as found in the initial MLR model to predict SB, were collinear, thereby demonstrating that the regression coefficients and *p* values may be biased. Due to the presence of collinearity, it was concluded that the MLR model defined in Tables 17 through 19 could not be used to properly interpret the relationships between the variables. The adjusted R^2 and standard error results to predict SE are presented in Table 17; the MLR Coefficients to predict SE are presented in Table 18; and the collinearity statistics to predict SE are presented in Table 19. Overall, Tables 17 through 19 summarize the MLR analysis results to predict SE.

Table 17. Adjusted R Square and Standard Error to Predict SE

Adjusted R^2	Standard Error of the Estimate
.657	.392

Table 18. MLR Coefficients to Predict SE

	β	*t*	*p*
Intercept	.158	.406	.686
MS	.029	.253	.801
SA	.565	6.592	.000***
SC	.329	2.938	.004**
CSE	.064	.919	.361

** $p < .05$, *** $p < .001$

Table 19. Collinearity Statistics to Predict SE

Variable	*VIF*
MS	2.763[a]
SA	1.519
SC	2.592[a]
CSE	1.008

Note. a indicates excessive collinearity.

To correct the MLR model for the influence of excessive collinearity, a new composite variable, MS x SC, was created. The MLR model to predict the dependent variable SE, including MS x SC, using standardized coefficients was:

SE = .864 + .569*SA + .069*CSE + .320*MS x SC + 0

The adjusted R^2 = .622 indicated that this model predicted a high proportion of the variance in SE. The value of $p < .05$ for the *t* statistics indicated that the intercept was not

zero and that SE increased significantly with respect to both SA and MS x SC. The *p* values > .05 for the *t* statistic indicated that the regression coefficients for CSE were not significantly different from zero, thus indicating that CSE was not a significant predictor of SE. Additionally, performing MLR analysis for the model with CSE removed produced the same adjusted R^2 = .622, providing further evidence that CSE did not contribute to the explanation of the variance in the dependent variable.

The revised MLR model to predict the dependent variable, SE, including MS x SC, did not violate the statistical assumptions of MLR with respect to excessive collinearity. The *VIF* statistics < 2.5 indicated that the independent variables MS (1.516), SA (1.511), and CSE (1.005) were not collinear, thereby demonstrating that the MLR statistics were not biased. The adjusted R^2 and standard error results to predict SE, including MS x SC, are presented in Table 20; the MLR coefficients to predict SE, including MS x SC, are presented in Table 21; and the collinearity statistics to predict SE, including MS x SC, are presented in Table 22. Overall, Tables 20 through 22 summarize the MLR analysis results to predict SE, including MS x SC.

Table 20. Adjusted R Square and Standard Error to Predict SE, Including MS x SC

Adjusted R Square	**Standard Error of the Estimate**
.622	.401

Table 21. MLR Coefficients to Predict SE, Including MS x SC

	β	***t***	***p***
Intercept	.864	2.394	.019*
SA	.569	6.524	.000***
MS x SC	.320	3.666	.000***
CSE	.069	.972	.334

*** p < .001
* p < .05

Table 22. Collinearity Statistics to Predict SE, Including MS x SC

Variable	***VIF***
SA	1.511
MS x SC	1.516
CSE	1.005

The approximately bell-shaped frequency distribution histogram visually indicated that the residuals for the MLR model to predict SE, including MS x SC, were normally distributed. The recalculated Kolmogorov Smirnov Z statistic = .903, p = .388 also confirmed residual normality. The residuals were somewhat evenly distributed around their mean (zero) value, reflecting heteroskedacity or differing variances. However, the residuals did not display a definitive wedge-shaped pattern, thus indicating that the variances did not evenly decrease with respect to an increase in the predicted values of SE. The revised MLR model was considered to be a good fit to the two independent

variables SA and CSE, the composite independent variable MS x SC, and the dependent variable SE. The author concluded that, by comparing the magnitudes of the revised MLR coefficients, SA (β = .569) was a more significant predictor of SE than was MS x SC (β = .320).

The adjusted R^2 value is an indicator of how well a regression model fits a set of data, and is computed from the ratio between the residual sum of squares and error sum of squares (SPSS, n.d.). The larger the adjusted R^2 value, the smaller is the variability of the residual values around the regression line relative to the overall variability, and the better is the fit of the data to the model (Hill & Lewicki, 2006). The smaller the adjusted R^2 value, the larger the variability of the residual values around the regression line relative to the overall variability, and the worse is the fit of the data to the model (Hill & Lewicki).

In this investigation, the adjusted R^2 = .622 for the model to predict SE including MS x SC had a higher value compared to the adjusted R^2 = .204 for the model to predict SB including MS x SC, inferring that the model to predict SE was a better fit to the data than the model to predict SB. The reason for this difference can be explained visually by observing the scatter plots of the standardized residuals versus the predicted values in Figures 10 and 11. There is a wider and more variable scatter of residuals either side of the mean (zero) line for the model to predict SB (Figure 10) than there is for the model to predict SE (Figure 11). The difference between the R-Squares of the two models was simply due to differences in the distribution patterns of their residuals. The distribution of residuals for the MLR model to predict SE, including MS x SC, is presented in Figure 11.

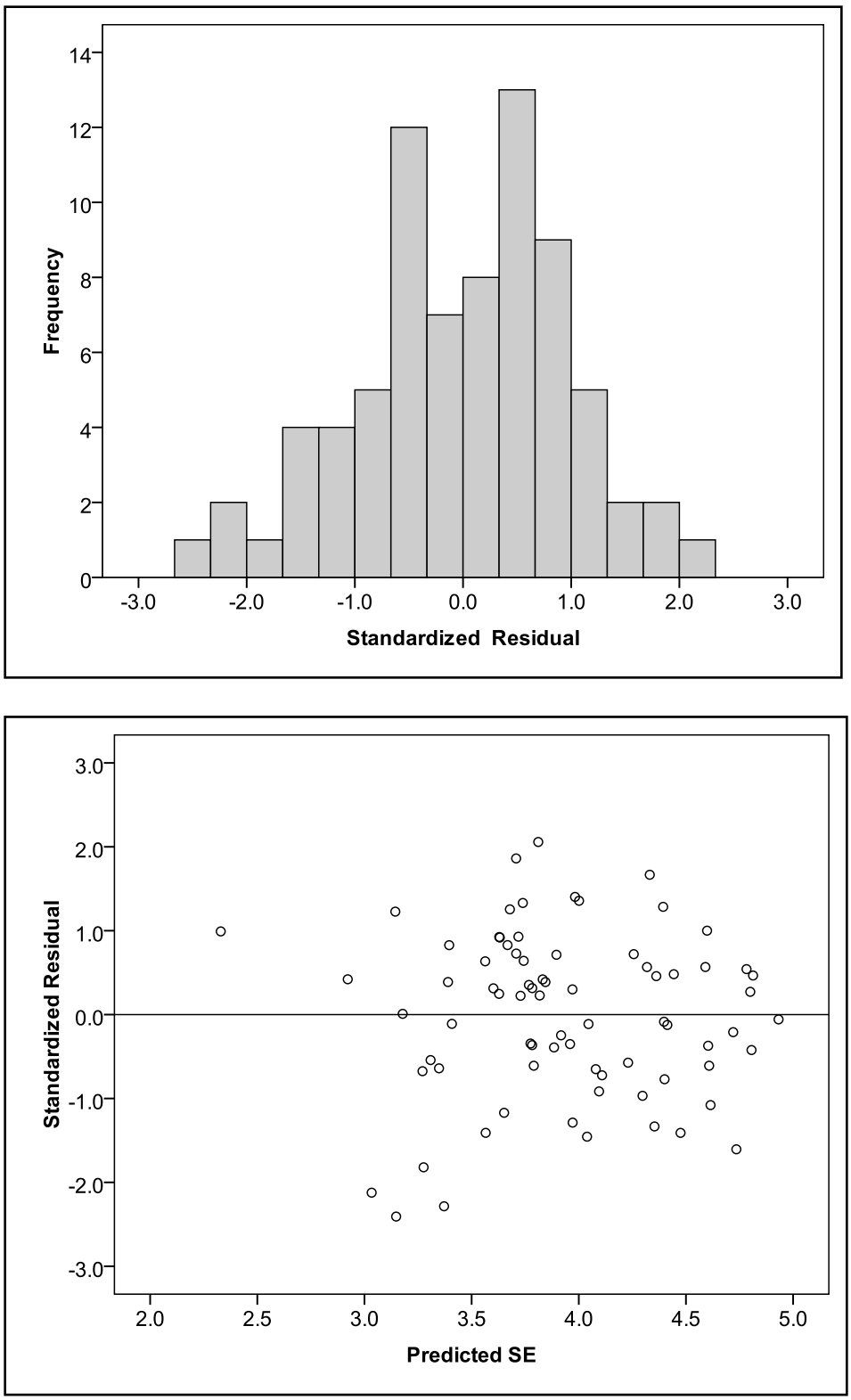

Figure 11. Distribution of residuals for the MLR model to predict SE, including MS x SC.

Results of Power Analysis

To investigate the minimum sample size in the study as a means to adequately permit the rejection of the null hypothesis of MLR, where the adjusted R^2 did not explain a substantial proportion of the variance in the dependent variable, the author performed a post-hoc power analysis. Cohen (1992) calculated the minimum sample sizes necessary to attain the desired power = 0.8 to reject the null hypothesis of MLR analysis at two specified significance levels (α = .01 or α = .05) and three population effect sizes ES = $(R^2)/(1 - R^2)$ for k = 2 to 8 independent variables**.** The threshold effect sizes were categorized as small (ES = .02), medium (ES = .15), and large (ES = .35). The values of N for small, medium, and large ES at Power = .80 for α = .01 and .05 are presented in Table 23.

Table 23. N for Small, Medium, and Large ES at Power = .80 for α = .01 and .05 (Cohen, 1992, p. 158)

	.01			**.05**		
Multi *R* Test	**Small**	**Medium**	**Large**	**Small**	**Medium**	**Large**
2k[b]	698	97	45	481	67	30
3k[b]	780	108	50	547	76	34
4k[b]	841	118	55	599	84	38
5k[b]	901	126	59	645	91	42
6k[b]	953	134	63	686	97	45
7k[b]	998	141	66	726	102	48
8k[b]	1039	147	69	757	107	50

Note. b indicates the number of independent variables.

For the two MLR models developed in this investigation to predict SB and SE, including MS x SC as a composite independent variable, the significance criterion was $\alpha = .05$ for $k = 3$ independent variables. The adjusted R^2 value for the MLR model to predict SB, including MS x SC, = .204, indicating that the effect size, $ES = (R^2)/(1 - R^2) = .256$ for $k = 3$ independent variables, was medium. Additionally, the adjusted R^2 value for the MLR model to predict SE, including MS x SC, = .633, indicating that the effect size $ES = (R^2)/(1 - R^2) = 1.725$ for $k = 3$ independent variables, was large. As noted in Table 27, when $\alpha = .05$ and $k = 3$, the minimum sample size should be $N = 76$, when the effect size is medium, and $N = 34$, when the effect size is large. Therefore, the sample size of 76 used in this investigation was adequate to reject the null hypothesis of MLR.

Summary of Results

This chapter presented the results of the statistical analyses used in the investigation. The results relevant to the six research questions showing the effect of management support, security awareness, security culture, and computer self-efficacy on secure behavior and security effectiveness, and thus HIPAA security compliance in AMCs, were presented. Prior to performing the statistical analyses, pre-analysis data screening was done to ensure the accuracy of the data collected from the Web-based survey. The pre-analysis data screening included testing for data accuracy, response-set, missing data, and multivariate outliers. Mahalanobis Distance (D^2) values were computed for all 76 cases and indicated that no outliers existed. The validity and reliability of the survey instrument were measured. Content validity, construct validity, and external validity measures were

assured by basing the survey items on previously validated scales from the literature. Cronbach's α reliability tests were performed for the independent and dependent variables to determine how well the survey items were internally consistent with each other. The results showed a high internal reliability for the items in each variable.

Following the pre-analysis data screening, as well as validity and reliability tests, descriptive statistics for the variables were calculated. These included the mean, standard deviation, Kolmogorov-Smirnov *Z* statistic, and significance. Frequency distribution histograms provided evidence that the variables were normally distributed. MLR and correlation analysis were performed to answer the five research questions of the study. Pearson correlation analysis and visual inspection of the matrix of scatter plots indicated that the relationship between the independent variables MS, SA, and SC and dependent variables SB and SE was linear, at $p < .01$.

The independent variable CSE was determined not to be significantly related to either of the dependent variables. The correlation analysis indicated that the independent variables MS, SA, and SC were collinear, thus violating the assumptions of MLR analysis. Using a second method, excessive collinearity between the independent variables MS and SC was confirmed by computing *VIF* statistics, thereby indicating that the existing MLR model could not properly interpret the relationships between the variables. As a result, MS and SC were combined to create a new composite independent variable (MS x SC). A revised MLR model was developed using SA, CSE, and the composite MS x SC variable to predict each of the SB and SE dependent variables, thus eliminating the problem of collinearity.

The revised MLR model to predict SB including MS x SC was:

SB = 3.311 + .265*SA - .122*CSE + .255*MS x SC

This model explained 20.4% of the variance in SB. It predicted that SB increased significantly at the .05 level, with respect to both MS x SC and SA. CSE was not a significant predictor of SB. The bell-shaped frequency histograms and Kolmogorov-Smirnov *Z* statistic confirmed that the residuals were normally distributed but exhibited slight heteroskedacity. The author concluded that, by comparing the magnitudes of the standardized regression coefficients, SA was a more significant predictor of SB than was MS x SC.

The revised MLR model to predict SE including MS x SC was:

SE = .864 + .569*SA + .069*CSE + .320*MS x SC

This model predicted a high proportion of the variance in SE, reflected by the adjusted R^2 = .622. SE increased significantly at the .05 level with respect to SA and MS x SC, while CSE was not a significant predictor of SE. This model did not violate the statistical assumptions of MLR with respect to residual normality or homogeneity of variance. The author concluded that, by comparing the magnitudes of the standardized regression coefficients, SA was a more important predictor of SE than was MS x SC.

Finally, to investigate the minimum sample size in the study to adequately permit the rejection of the null hypothesis of MLR, a post-hoc power analysis was performed. The adjusted R^2 value for the MLR model used to predict SB, using MS x SC, was medium, indicating that a sample size of N = 76 was sufficient. The adjusted R^2 value for the MLR model used to predict SE, using MS x SC, was large, indicating a sample size of N = 34 was needed. Therefore, the sample size of 76 used in this investigation was adequate to reject the null hypothesis of MLR.

Chapter 5

Conclusion, Implications, Recommendations, and Summary

Conclusion

The research problem that the author investigated concerned the fact that AMCs and other covered entities in the U.S. are not fully complying with HIPAA. The main goal of the study was to assess and empirically validate a theoretical model that uses management support, security awareness, security culture, and computer self-efficacy to predict security behavior and security effectiveness and thus HIPAA security compliance in AMCs. To empirically assess the effect of the above-noted variables on HIPAA security compliance in AMCs, a Web-based survey using previously validated scales was developed. The target population of this investigation was health care professionals associated with the AAMC. The target sample of this study was health care professionals who are members of the GIR within the AAMC. From a total membership of approximately 590 IT professionals in the GIR, 76 individuals responded to the survey, yielding a response rate of 12.9%.

The main research question that this study addressed was: What is the effect of management support, security awareness, security culture, and computer self-efficacy on security behavior and security effectiveness and thus HIPAA security compliance in AMCs? MLR analysis results demonstrated that the theoretical model of this investigation predicted security effectiveness 62.2% of the time. MLR analysis also showed that the model predicted security behavior 20.4% of the time. Pearson correlation analysis revealed that MS, SA, and SC were collinear. As a result, a new composite

variable, MS x SC, was developed. Consequently, MLR analysis indicated that the independent variables SA and MS x SC had a significant effect on the dependent variables, SE and SB. CSE, however, did not have a significant effect on either dependent variable.

The main research question of this investigation can be understood as consisting of four specific research questions. The first research question was: What is the effect of management support on security behavior and security effectiveness and thus HIPAA security compliance in AMCs? The management support construct has been applied minimally in the fields of IT and information security research but has not been applied within the context of an academic medical environment. Therefore, this investigation identified a new construct: management support and its effect on security effectiveness and security behavior and thus HIPAA security compliance in AMCs. The findings of MLR and correlation analyses demonstrated that management support, when associated with security culture, had a strong weight in predicting HIPAA security compliance. The author's findings empirically validated the research reported in the literature by Barry and Grossmeier (2009), Logan and Noles (2008), and Loghry and Veach (2009) that management support is a significant construct that affects HIPAA security compliance.

The second research question was: What is the effect of security awareness on security behavior and security effectiveness and thus HIPAA security compliance in AMCs? The security awareness construct has been applied minimally in the fields of IT and information security research but has not been applied within the context of an academic medical environment. Therefore, this investigation identified a new construct: security awareness and its effect on security effectiveness and security behavior and thus HIPAA

security compliance in AMCs. The findings of MLR and correlation analyses demonstrated that security awareness had the strongest weight in predicting HIPAA security compliance. The author's findings empirically validated the research reported in the literature by Lending and Dillon (2007), Medlin and Cazier (2007), and North et al. (2009) that security awareness is an important construct that affects HIPAA security compliance.

The third research question was: What is the effect of security culture on security behavior and security effectiveness and thus HIPAA security compliance in AMCs? The security culture construct has been applied minimally in the fields of IT and information security research but has not been applied within the context of an academic medical environment. Therefore, this investigation identified a new construct: security culture and its effect on security effectiveness and security behavior and thus HIPAA security compliance in AMCs. The findings of MLR and correlation analyses demonstrated that security culture, when associated with management support, had a strong weight in predicting HIPAA security compliance. The author's findings provided additional support for the findings reported in the literature by Lineberry (2007), Ma et al. (2008), and Sveen et al. (2007) that security culture is a significant construct that affects HIPAA security compliance.

The fourth research question was: What is the effect of computer self-efficacy on security behavior and security effectiveness and thus HIPAA security compliance in AMCs? The computer self-efficacy construct has been applied minimally in the fields of IT and information security research but has not been applied within the context of an academic medical environment. Therefore, this investigation identified a new construct:

computer self-efficacy and its effect on security effectiveness and security behavior and thus HIPAA security compliance in AMCs. The findings of MLR and correlation analyses indicated that computer self-efficacy did not have a strong weight in predicting HIPAA security compliance. Although the findings reported in the literature by Chan et al. (2005), Lending and Dillon (2007), and Womble (2008) assert that computer self-efficacy is a significant construct that affects HIPAA security compliance, the author's findings provide additional evidence that more research on the factors associated with self-efficacy is warranted (Ball & Levy, 2008; Lending & Dillon). The empirically-validated conceptual model of the relevant factors and their effects on HIPAA security compliance in AMCs is presented in Figure 12.

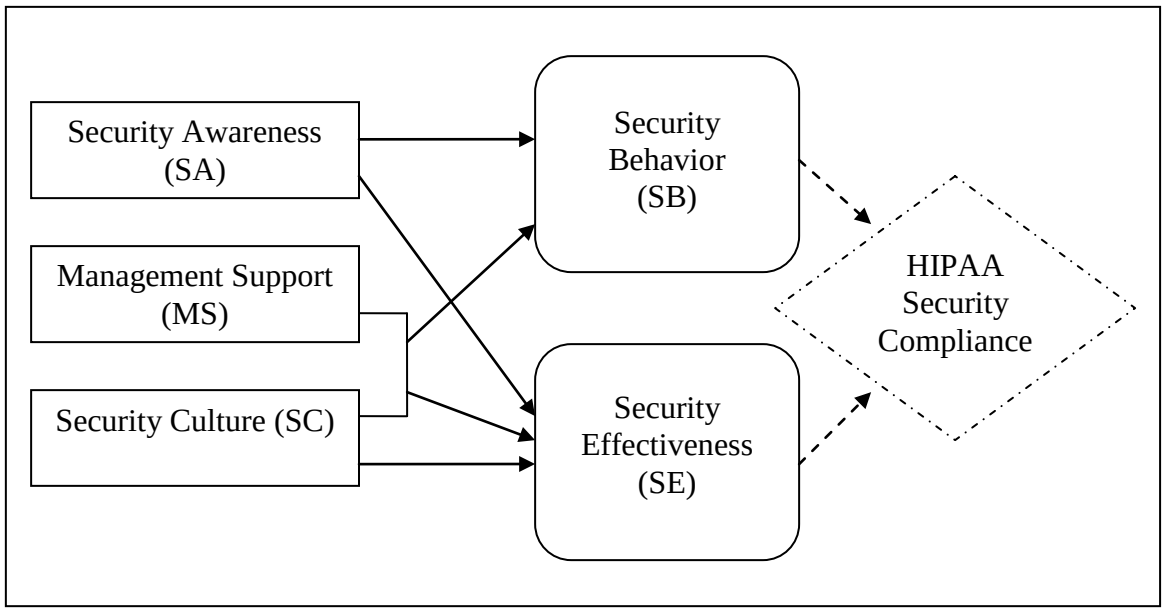

Figure 12. The empirically-validated conceptual model of the relevant factors and their effects on HIPAA security compliance in AMCs.

Implications

The implications of this investigation for research are significant. The author developed a theoretical model using the variables of management support, security

awareness, security culture, and computer self-efficacy to predict security effectiveness and security behavior and thus HIPAA security compliance in AMCs. The independent and dependent variables selected for the model were based on a comprehensive literature search by the author. As a result, the two main contributions that this investigation makes to the technology acceptance and security effectiveness literature include: (a) the development and empirical validation of a theoretical model for predicting security effectiveness and security behavior and thus HIPAA security compliance in AMCs; and (b) the determination of the most significant factors that affect security effectiveness and security behavior and thus HIPAA security compliance in AMCs. These findings should help facilitate the understanding of HIPAA security compliance among AMCs.

The implications of this investigation for practice are threefold. First, the results of this study provide guidance for the individuals and organizations associated with AMCs who are involved with HIPAA security compliance initiatives in the health care domain. The findings of this study contribute knowledge that can be applied to improve information security and regulatory compliance in the HIPAA domain, with a focus on AMCs. Second, this investigation provides valuable information that can be used in AMCs to (a) decrease data security breaches; (b) improve security measures required by the increased use of IT in health care; (c) better prepare for the stricter enforcement and increased federal audits of HIPAA Security Rule compliance; and (d) improve compliance with the new federal regulations extending the HIPAA Security Rule. Finally, the research model developed as an outcome of this investigation can help information security researchers and practitioners understand the variety of factors affecting the current HIPAA security requirements as implemented by AMCs. With this study and the existing body of

knowledge, AMCs and health care organizations will be better able to understand and comply with the HIPAA Security Rule.

Limitations

In this study, four limitations were identified. First, the participants of this study were members of the AAMC GIR, which included IT professionals from medical schools, teaching hospitals and health systems, and academic and professional societies. Therefore, the generalizability of this investigation might be limited only to health care organizations that are considered AMCs. Additional studies need to be done at non-AMC health care organizations to be able to more broadly generalize the findings of this study.

Second, the survey for this investigation was completed within a 4-week period. With the recent addition of new federal and state regulations modifying HIPAA security compliance requirements through the year 2015, increased audits of HIPAA security compliance, and stricter enforcement of penalties for noncompliance of the HIPAA Security Rule, a longitudinal study may be needed to measure the effect of management support, security awareness, security culture, and computer self-efficacy on security effectiveness and security behavior over time. AMCs must periodically reassess their compliance to the HIPAA Security Rule as the various compliance dates become effective.

Third, the data collected by the author was self-reported. The investigation did not measure actual HIPAA security compliance. Therefore, the reliability of the survey data was dependent on the AAMC GIR members' truthfulness and ability to report their perceptions of security without bias, preconceived notions, or reluctance to report

security shortcomings. In additional, the survey responses were checked for data accuracy, response-set, missing data, and outliers to reduce the self-report bias.

Finally, the Web-based survey instrument was distributed to the respondents through e-mail with no special incentive given to the respondents to complete the survey. To increase the response rate, the survey deadline was extended from April 22, 2010, to May 7, 2010. In addition, two reminders to complete the survey were e-mailed to the AAMC GIR members. The respondents' willingness to self-select and dedicate the necessary time to complete the survey may have contributed to the limited the number of surveys completed. Based on this self-selection, there may have been an under-representation of IT professionals who are not concerned about HIPAA security compliance.

Recommendations

Several areas of future research were identified. The author did not restrict the current study to one AMC per respondent. Thus, future investigations could ensure that no more than one representative from each AAMC organization participates in the survey. Future studies could also explore whether HIPAA security compliance perceptions differ based on the AAMC GIR member role in their organization. In addition, researching the perceptions of HIPAA security compliance from a broader group of health care professions (e.g., executives, line management, financial, clinical, and technical) within a single AMC would provide a richer view of differences in security compliance within an organization.

Requesting respondents to confirm that they have sufficient knowledge of their organization's information security program could be required in subsequent studies. The current study assumed that, because the AAMC GIR members were IT professionals, the

respondents had an acceptable and working understanding of their organization's IT and information security program. Replicating this investigation to include a wider range of health care organizations that are not included in AMCs, such as health maintenance organizations, physician practice groups, hospital networks, independent practice associations, physician sponsored networks, managed care organizations, clinics, practice management firms, and preferred provider organizations, would increase the generalizability of the findings.

Examining additional factors affecting HIPAA security compliance from the literature, such as security framework (Moreira et al., 2008; Thomas & Botha, 2007), perceived security (Lallmahamood, 2007), perceived usefulness of security (Novakovic et al., 2009), resistance to change (Smith & Jamieson, 2006), and trust (Kim & Ahn, 2007), also could be considered in future research. To ensure that the present study remained manageable, these additional variables were not investigated. Therefore, this investigation was not an exhaustive study of all factors that affect HIPAA security compliance.

This study examined the effect of the independent variables, MS, SA, SC, and CSE, on the dependent variables, SE and SB, and thus HIPAA security compliance in AMCs. However, actual HIPAA security compliance was not measured. Future investigations could measure actual HIPAA security compliance in AMCs.

Finally, the results of this investigation indicated that health care leadership in AMCs, represented in part by the AAMC GIR members, acknowledged that management support, security awareness, and security culture are important factors in attaining HIPAA security compliance. Computer self-efficacy was not reported as a significant

factor affecting HIPAA security compliance. The literature has reported that AMCs are not fully complying with the HIPAA Security Rule and that a better understanding of management support, security awareness, security culture, and computer self-efficacy is needed. Future research examining factors affecting management support, security awareness, security culture, and computer self-efficacy in practice could result in knowledge to help ensure improved HIPAA security compliance.

Summary

This investigation addressed the research problem that AMCs and other covered entities in the U.S. are not fully complying with HIPAA (Hasemyer, 2009; Herold, 2009a; Holland, 2009). According to Herold (2009b), data security breaches in health care organizations continue to increase. Numerous AMCs have recently reported data security breaches (DataLossDB, 2010; Privacy Rights Clearinghouse, 2010). The rapid growth and use of information technology has created new security issues in health care organizations (Connell & Young, 2007; Helms et al., 2008; Thomas & Botha, 2007). According to Logan and Noles (2008), Ma et al. (2008), and Nash (2008), numerous health care organizations have been reactive in addressing these new security concerns. Shortcomings in the HIPAA Security Rule relating to business associates, breach notifications, data transmission standards, investigation of complaints, and penalties and enforcement have created liabilities for health care organizations (Brown, 2009a, 2009b; Blades, 2009). As a consequence, Hourihan (2009) and Ruzic (2009) indicated that the federal government has implemented stringent HIPAA security compliance reviews. In

addition, new regulations and legislation have significantly extended the scope and enforcement of the HIPAA Security Rule (Bianchi, 2009; Hourihan; Rath, 2009).

Based on a comprehensive review of the literature of technology acceptance and security effectiveness, a theoretical model was developed to predict the effect of management support, security awareness, security culture, and computer self-efficacy on security behavior and security effectiveness and thus HIPAA security compliance in AMCs. Prior investigations by Barry and Grossmeier (2009), Logan and Noles (2008), and Loghry and Veach (2009) viewed management support as a significant determinant of security compliance. According to Lending and Dillon (2007), Medlin and Cazier (2007), and North et al. (2009), security awareness is a critical factor in attaining HIPAA security compliance. Security culture is another factor that plays a significant role in information security management (Lineberry, 2007; Ma et al., 2008; Sveen et al., 2007). According to Chan et al. (2005), Lending and Dillon, and Womble (2008), computer self-efficacy is another factor that is a significant predictor of security compliance behavior. Therefore, management support, security awareness, security culture, and computer self-efficacy are important factors in HIPAA security compliance. In addition, D'Arcy and Hovav (2009), Hazari et al. (2008), and Jahankhani et al. (2007) concluded that security effectiveness is a valid predictor of security behavior, while Filipek (2007), Hazari et al., and Pattison and Anderson (2007) found that security behavior influenced security effectiveness.

The goal of the study was to develop a model, as was presented in Figure 1, based on the analysis of the effect of management support, security awareness, security culture, and computer self-efficacy on security behavior and security effectiveness and thus

HIPAA security compliance in AMCs. The main research question that this study addressed was: What is the effect of management support, security awareness, security culture, and computer self-efficacy on security behavior and security effectiveness and thus HIPAA security compliance in AMCs? This investigation also addressed the following four specific research questions:

1. What is the effect of management support on security behavior and security effectiveness and thus HIPAA security compliance in AMCs? (Barry & Grossmeier, 2009; Logan & Noles, 2008; Loghry & Veach, 2009).

2. What is the effect of security awareness on security behavior and security effectiveness and thus HIPAA security compliance in AMCs? (Lending & Dillon, 2007; Medlin & Cazier, 2007; North et al., 2009).

3. What is the effect of security culture on security behavior and security effectiveness and thus HIPAA security compliance in AMCs? (Lineberry, 2007; Ma et al., 2008; Sveen et al., 2007).

4. What is the effect of computer self-efficacy on security behavior and security effectiveness and thus HIPAA security compliance in AMCs? (Chan et al., 2005; Lending & Dillon, 2007; Womble, 2008).

The target population of this investigation was health care professionals associated with the AAMC. The sample for this empirical study was health care information technology professionals who are members of the GIR within the AAMC. In this study, the author developed a 61-item Web-based survey, which used Likert-scaled multiple items to determine the factors affecting HIPAA security compliance in AMCs. The survey was developed using a combination of existing and validated scales.

Six items for management support in the instrument, MS1 to MS6, were adapted from the survey items developed and validated by Knapp et al. (2007); and four items for management support in the instrument, MS7 to MS10, were adapted from the survey items developed and validated by Lin (2007). Four items for SA in the instrument, SA1 to SA4, were developed by consolidating and adapting survey items developed and validated by D'Arcy and Hovav (2009); four items for SA in the instrument, SA5 to SA8, were developed by consolidating and adapting survey items developed and validated by Knapp et al. (2007); and two items for SA in the instrument, SA9 and SA10, were developed by consolidating and adapting survey items developed and validated by Johnston and Warkentin (2008). Six items for SC in the instrument, SC1 to SC6, were adapted from the survey items developed and validated by Knapp et al. (2007); and four items for SC in the instrument, SC7 to SC10, were adapted from the survey items developed and validated by Chan et al. (2005).

Ten items for CSE in the survey, CSE1 to CSE10, were adapted from the survey items developed and validated by Ball and Levy (2008). Five items for SB in the instrument, SB1 to SB5, were developed by consolidating and adapting survey items developed and validated by Chan et al. (2005); one item for SB in the instrument, SB6, was developed by consolidating and adapting a survey item developed and validated by Cazier et al. (2007); three items for SB in the instrument, SB7 to SB9, were developed by consolidating and adapting survey items developed and validated by Hazari et al. (2008); and one item for SB in the instrument, SB10, was developed by consolidating and adapting a survey item developed and validated by Johnston and Warkentin (2008). Finally, five items for security effectiveness in the instrument, SE1 to SE5, were adapted

from the survey items developed and validated by Knapp et al. (2007); and six items for security effectiveness in the instrument, SE6 to SE11, were adapted from the survey items developed and validated by Chang and Lin (2007).

Two statistical methods, MLR and correlation analysis, were used to test the conceptual research model of this investigation. The theoretical model predicted that MS, SA, SC, and CSE would have a significant effect on SE and SB and thus HIPAA security compliance in AMCs. A total of 590 AMC GIR members participated in the Web-based survey, representing a 12.9% response rate. The results of the investigation demonstrated that SA and MS x SC were significant predictors of the dependent variables, SE and SB, in the MLR model. CSE was not a significant predictor of either dependent variable. MLR analysis indicated that the SA and the composite MS x SC independent variables accounted for 20.4% of the variance in the dependent variable SB and that SB increased significantly with respect to both SA and MS x SC. MLR analysis also indicated that the SA and the composite MS x SC independent variables accounted for 62.2% of the variance in the dependent variable SE and that SE increased significantly with respect to both SA and MS x SC. SA was a more significant predictor of SB and SE than was MS x SC.

Finally, a power analysis was performed to validate that the sample size of 76 used in this investigation was adequate to reject the null hypothesis of MLR. Following MLR analysis, the results of the investigation were reviewed. Conclusions were discussed and correlated to the technology acceptance and security effectiveness literature. Theoretical and practical implications of the study were defined. Four limitations of the investigation were identified and summarized. Finally, recommendations were presented for future

research that will build upon the author's research and extend the body of knowledge in the area of HIPAA security compliance in AMCs.

Appendix A

Survey

Dear GIR Member,

As a Ph.D. student in the Graduate School of Computer and Information Sciences at Nova Southeastern University, I am conducting research for my doctoral dissertation that will investigate factors affecting HIPAA security compliance in academic medical centers. HIPAA security compliance in academic medical centers is a central concern of researchers, academicians, and practitioners. Data security breaches are increasing globally, causing concern over the confidentiality, integrity, and availability of electronic personal health information. As health care organizations strive to implement electronic health records, the growth of information technology has created new security issues. The federal government has recently implemented stringent HIPAA security compliance reviews. In addition, the passage of the Health Information Technology for Economic and Clinical Health Act on February 17, 2009, a part of the American Recovery and Reinvestment Act of 2009 has substantially altered and extended the HIPAA Security Rule compliance requirements.

As a result, I have developed a brief questionnaire to be used in an anonymous, Web-based survey. The survey instrument is designed to better understand the issues that influence HIPAA security compliance. The findings will contribute to the body of knowledge regarding factors affecting HIPAA security compliance in academic medical centers.

Prior to beginning the survey, please read the study information that follows. This information will outline your rights as a research participant. If you have any questions, please feel free to contact me by e-mail or cell phone listed below. Your participation in this survey is extremely important. I would appreciate you taking the time (approximately 20 minutes) to complete and submit this online survey by **April 22, 2010.**

The survey questions are about your perception towards HIPAA security compliance. Therefore, there is no right or wrong answer. Please, respond to the questions by choosing the answer that best represents your perception about the item.

Please click on http://www.surveymonkey.com/s/VD7HPVD to begin the survey. Thank you very much for your support!

Sincerely,

James W. Brady, M.S., M.Ed.
Health System Manager
Enterprise Information Services
Cedars-Sinai Medical Center
Los Angeles, CA 90048
310-924-5785
James.Brady@cshs.org

Study Information

What is this study about?

As a member of the AAMC's Group on Information Resources, you are being invited to participate in research to determine the factors that affect HIPAA security compliance in academic medical centers.

What do I need to do to participate in this study?

You will need approximately 20 minutes to complete the online survey questions.

What are the risks and benefits of this study?

There are no foreseeable risks associated with this investigation. Although there are no direct personal benefits for participating in this study, you will be enhancing the general understanding of factors that affect HIPAA security compliance in academic medical centers.

Are there any costs and payments involved with this study?

There are no costs or payments for your participation in this study. Although there is no compensation for your participation, the results of the study may provide guidance to those individuals and organizations involved with HIPAA security-compliance initiatives in health care.

How will my survey responses be kept confidential and private?

As a participant of this research, please understand that your anonymity will be protected. Your responses will be delivered to me in a database that will include no means of identifying respondents. The data collected in this study are anonymous and all your responses will be kept strictly confidential. Only the summary of the results will be communicated to all participants as well as your organization upon request.

What if I do not want to participate or I want to leave the study?

You have the right to exit the survey questionnaire at any time or refuse to participate. If you are uncomfortable with any questions, you may end the survey at any point.

Is my participation in this study voluntary?

Your participation is strictly voluntary. You are under no obligation to participate in this investigation. By completing and submitting the Web-based survey, you are agreeing to voluntarily participate in this investigation.

Survey

1. The following is a list of statements related to the influence of management support on HIPAA security compliance at your organization. Please read each item and rate the level of agreement you attribute to each statement from: (1) 'Strongly Disagree' to (5) 'Strongly Agree'.

	Items	Strongly Disagree	Disagree	Neither Disagree Nor Agree	Agree	Strongly Agree
		1	2	3	4	5
MS1:	Top management considers HIPAA security compliance an important organizational priority in my organization.	1 [ ]	2 [ ]	3 [ ]	4 [ ]	5 [ ]
MS2:	Top executives are interested in HIPAA security compliance issues in my organization.	1 [ ]	2 [ ]	3 [ ]	4 [ ]	5 [ ]
MS3:	Top management takes HIPAA security compliance issues into account when planning corporate strategies in my organization.	1 [ ]	2 [ ]	3 [ ]	4 [ ]	5 [ ]
MS4:	Senior leadership's words and actions demonstrate that HIPAA security compliance is a priority in my organization.	1 [ ]	2 [ ]	3 [ ]	4 [ ]	5 [ ]
MS5:	Visible support for HIPAA security compliance goals by senior management is obvious in my organization.	1 [ ]	2 [ ]	3 [ ]	4 [ ]	5 [ ]

1. The following is a list of statements related to the influence of management support on HIPAA security compliance at your organization. Please read each item and rate the level of agreement you attribute to each statement from: (1) 'Strongly Disagree' to (5) 'Strongly Agree'.

	Items	Strongly Disagree	Disagree	Neither Disagree Nor Agree	Agree	Strongly Agree
		1	2	3	4	5
MS6:	Senior management gives strong and consistent support to my organization's HIPAA security compliance program in my organization.	1 [ ]	2 [ ]	3 [ ]	4 [ ]	5 [ ]
MS7:	Top managers think that HIPAA security compliance is beneficial in my organization.	1 [ ]	2 [ ]	3 [ ]	4 [ ]	5 [ ]
MS8:	Top managers always support and encourage employees complying with HIPAA security requirements in my organization.	1 [ ]	2 [ ]	3 [ ]	4 [ ]	5 [ ]
MS9:	Top managers provide most of the necessary help and resources to enable employees to comply with HIPAA security requirements in my organization.	1 [ ]	2 [ ]	3 [ ]	4 [ ]	5 [ ]
MS10:	Top managers are keen to see that the employees are happy to comply with HIPAA security requirements in my organization.	1 [ ]	2 [ ]	3 [ ]	4 [ ]	5 [ ]

2. The following is a list of statements related to the influence of security awareness on HIPAA security compliance at your organization. Please read each item and rate the level of agreement you attribute to each statement from: (1) 'Strongly Disagree' to (5) 'Strongly Agree'.

	Items	Strongly Disagree	Disagree	Neither Disagree Nor Agree	Agree	Strongly Agree
		1	2	3	4	5
SA1:	My organization provides HIPAA security awareness training to help employees improve their awareness of computer and information security issues.	1 [ ]	2 [ ]	3 [ ]	4 [ ]	5 [ ]
SA2:	In my organization, employees are briefed on the consequences of modifying computerized data in an unauthorized way.	1 [ ]	2 [ ]	3 [ ]	4 [ ]	5 [ ]
SA3:	My organization educates employees on their computer security responsibilities.	1 [ ]	2 [ ]	3 [ ]	4 [ ]	5 [ ]
SA4:	In my organization, employees are briefed on the consequences of accessing computer systems that they are not authorized to use.	1 [ ]	2 [ ]	3 [ ]	4 [ ]	5 [ ]
SA5:	An effective HIPAA security awareness program exists at my organization.	1 [ ]	2 [ ]	3 [ ]	4 [ ]	5 [ ]

2. The following is a list of statements related to the influence of security awareness on HIPAA security compliance at your organization. Please read each item and rate the level of agreement you attribute to each statement from: (1) 'Strongly Disagree' to (5) 'Strongly Agree'.

	Items	Strongly Disagree	Disagree	Neither Disagree Nor Agree	Agree	Strongly Agree
		1	2	3	4	5
SA6:	A continuous, ongoing HIPAA security awareness program exists at my organization.	1 [ ]	2 [ ]	3 [ ]	4 [ ]	5 [ ]
SA7:	Users receive adequate HIPAA security awareness refresher training appropriate for their job function at my organization.	1 [ ]	2 [ ]	3 [ ]	4 [ ]	5 [ ]
SA8:	HIPAA security awareness is an ongoing focus at my organization	1 [ ]	2 [ ]	3 [ ]	4 [ ]	5 [ ]
SA9:	HIPAA security awareness training is of sufficient length at my organization.	1 [ ]	2 [ ]	3 [ ]	4 [ ]	5 [ ]
SA10:	HIPAA security awareness training at my organizations helps me see the usefulness of following certain procedures to safeguard patient privacy.	1 [ ]	2 [ ]	3 [ ]	4 [ ]	5 [ ]

3. The following is a list of statements related to the influence of security culture on HIPAA security compliance at your organization. Please read each item and rate the level of agreement you attribute to each statement from: (1) 'Strongly Disagree' to (5) 'Strongly Agree'.

	Items	Strongly Disagree	Disagree	Neither Disagree Nor Agree	Agree	Strongly Agree
		1	2	3	4	5
SC1:	Employees at my organization value the importance of security.	1 [ ]	2 [ ]	3 [ ]	4 [ ]	5 [ ]
SC2:	A culture exists at my organization that promotes good security practices.	1 [ ]	2 [ ]	3 [ ]	4 [ ]	5 [ ]
SC3:	Security has traditionally been considered an important organizational value at my organization.	1 [ ]	2 [ ]	3 [ ]	4 [ ]	5 [ ]
SC4:	Practicing good security is the accepted way of doing business at my organization.	1 [ ]	2 [ ]	3 [ ]	4 [ ]	5 [ ]
SC5:	The overall environment at my organization fosters security-minded thinking.	1 [ ]	2 [ ]	3 [ ]	4 [ ]	5 [ ]
SC6:	Information security at my organization is a key norm shared by my fellow employees.	1 [ ]	2 [ ]	3 [ ]	4 [ ]	5 [ ]
SC7:	My organization sets high standards for the protection of its information assets.	1 [ ]	2 [ ]	3 [ ]	4 [ ]	5 [ ]

3. The following is a list of statements related to the influence of security culture on HIPAA security compliance at your organization. Please read each item and rate the level of agreement you attribute to each statement from: (1) 'Strongly Disagree' to (5) 'Strongly Agree'.

	Items	Strongly Disagree	Disagree	Neither Disagree Nor Agree	Agree	Strongly Agree
		1	2	3	4	5
SC8:	Management at my organization is concerned with information security.	1 [ ]	2 [ ]	3 [ ]	4 [ ]	5 [ ]
SC9:	My immediate supervisor is concerned with information security for the organization.	1 [ ]	2 [ ]	3 [ ]	4 [ ]	5 [ ]
SC10:	My coworkers are concerned with information security for the organization.	1 [ ]	2 [ ]	3 [ ]	4 [ ]	5 [ ]

4. The following is a list of statements related to the influence of self-efficacy on HIPAA security compliance at your organization. Please read each item and rate the level of agreement you attribute to each statement from: (1) 'Strongly Disagree' to (5) 'Strongly Agree'.

	Items	Strongly Disagree	Disagree	Neither Disagree Nor Agree	Agree	Strongly Agree
		1	2	3	4	5
CSE1:	I could comply with HIPAA security requirements at my organization if I had seen someone else complying with it before trying it myself.	1 [ ]	2 [ ]	3 [ ]	4 [ ]	5 [ ]
CSE2:	I could comply with HIPAA security requirements at my organization if I could call someone for help if I got stuck.	1 [ ]	2 [ ]	3 [ ]	4 [ ]	5 [ ]
CSE3:	I could comply with HIPAA security requirements at my organization if someone else had helped me get started.	1 [ ]	2 [ ]	3 [ ]	4 [ ]	5 [ ]
CSE4:	I could comply with HIPAA security requirements at my organization if I had a lot of time to complete the requirements.	1 [ ]	2 [ ]	3 [ ]	4 [ ]	5 [ ]

4. The following is a list of statements related to the influence of self-efficacy on HIPAA security compliance at your organization. Please read each item and rate the level of agreement you attribute to each statement from: (1) 'Strongly Disagree' to (5) 'Strongly Agree'.

	Items	Strongly Disagree	Disagree	Neither Disagree Nor Agree	Agree	Strongly Agree
		1	2	3	4	5
CSE5:	I could comply with HIPAA security requirements at my organization if someone showed me how to comply first.	1 [ ]	2 [ ]	3 [ ]	4 [ ]	5 [ ]
CSE6:	I could comply with HIPAA security requirements at my organization if there was no one around to tell me what to do as I go.	1 [ ]	2 [ ]	3 [ ]	4 [ ]	5 [ ]
CSE7:	I could comply with HIPAA security requirements at my organization if I had never tried complying before.	1 [ ]	2 [ ]	3 [ ]	4 [ ]	5 [ ]
CSE8:	I could comply with HIPAA security requirements at my organization if I had only written instructions for reference.	1 [ ]	2 [ ]	3 [ ]	4 [ ]	5 [ ]
CSE9:	I could comply with HIPAA security requirements at my organization if I was able to first see someone else complying.	1 [ ]	2 [ ]	3 [ ]	4 [ ]	5 [ ]

4. The following is a list of statements related to the influence of self-efficacy on HIPAA security compliance at your organization. Please read each item and rate the level of agreement you attribute to each statement from: (1) ‘Strongly Disagree’ to (5) ‘Strongly Agree’.

	Items	Strongly Disagree	Disagree	Neither Disagree Nor Agree	Agree	Strongly Agree
		1	2	3	4	5
CSE10:	I could comply with HIPAA security requirements at my organization if I could call someone for help if I needed help.	1 [ ]	2 [ ]	3 [ ]	4 [ ]	5 [ ]

5. The following is a list of statements related to the influence of secure behavior on HIPAA security compliance at your organization. Please read each item and rate the level of agreement you attribute to each statement from: (1) 'Strongly Disagree' to (5) 'Strongly Agree'.

	Items	Strongly Disagree	Disagree	Neither Disagree Nor Agree	Agree	Strongly Agree
		1	2	3	4	5
SB1:	I will comply with HIPAA security procedures at my organization when performing my daily work.	1 [ ]	2 [ ]	3 [ ]	4 [ ]	5 [ ]
SB2:	I tend to ignore HIPAA security procedures at my organization that I think are not necessary (reverse).	1 [ ]	2 [ ]	3 [ ]	4 [ ]	5 [ ]
SB3:	I tend to ignore HIPAA security procedures at my organization in order to complete my work quickly (reverse).	1 [ ]	2 [ ]	3 [ ]	4 [ ]	5 [ ]
SB4:	Sometimes I comply with HIPAA security procedures at my organization when it affects the performance/productivity of my work (reverse).	1 [ ]	2 [ ]	3 [ ]	4 [ ]	5 [ ]
SB5:	I tend to comply with HIPAA security procedures at my organization only when it is convenient to do so (reverse).	1 [ ]	2 [ ]	3 [ ]	4 [ ]	5 [ ]

5. The following is a list of statements related to the influence of secure behavior on HIPAA security compliance at your organization. Please read each item and rate the level of agreement you attribute to each statement from: (1) 'Strongly Disagree' to (5) 'Strongly Agree'.

	Items	Strongly Disagree	Disagree	Neither Disagree Nor Agree	Agree	Strongly Agree
		1	2	3	4	5
SB6:	Exhibiting good security behavior is rewarded at my organization.	1 [ ]	2 [ ]	3 [ ]	4 [ ]	5 [ ]
SB7:	I intend to continue complying with HIPAA security requirements at my organization.	1 [ ]	2 [ ]	3 [ ]	4 [ ]	5 [ ]
SB8:	I intend to increase my compliance with HIPAA security requirements at my organization.	1 [ ]	2 [ ]	3 [ ]	4 [ ]	5 [ ]
SB9:	I predict I will comply with HIPAA security requirements at my organization.	1 [ ]	2 [ ]	3 [ ]	4 [ ]	5 [ ]
SB10:	I plan to continue to safeguard patient and security at my organization.	1 [ ]	2 [ ]	3 [ ]	4 [ ]	5 [ ]

6. The following is a list of statements related to the influence of security effectiveness on HIPAA security compliance at your organization. Please read each item and rate the level of agreement you attribute to each statement from: (1) 'Strongly Disagree' to (5) 'Strongly Agree'.

	Items	Strongly Disagree	Disagree	Neither Disagree Nor Agree	Agree	Strongly Agree
		1	2	3	4	5
SE1:	My organization's HIPAA security program achieves most of its goals.	1 [ ]	2 [ ]	3 [ ]	4 [ ]	5 [ ]
SE2:	My organization's HIPAA security program accomplishes its most important objectives.	1 [ ]	2 [ ]	3 [ ]	4 [ ]	5 [ ]
SE3:	Generally speaking, my organization's ePHI is sufficiently protected.	1 [ ]	2 [ ]	3 [ ]	4 [ ]	5 [ ]
SE4:	Overall, my organization's HIPAA security program is effective.	1 [ ]	2 [ ]	3 [ ]	4 [ ]	5 [ ]
SE5:	My organization's HIPAA security program has kept risks to a minimum.	1 [ ]	2 [ ]	3 [ ]	4 [ ]	5 [ ]
SE6:	My organization enforces security controls (such as encryption of data in transit and at rest) to protect sensitive information and proprietary/business secrets.	1 [ ]	2 [ ]	3 [ ]	4 [ ]	5 [ ]

6. The following is a list of statements related to the influence of security effectiveness on HIPAA security compliance at your organization. Please read each item and rate the level of agreement you attribute to each statement from: (1) 'Strongly Disagree' to (5) 'Strongly Agree'.

	Items	Strongly Disagree	Disagree	Neither Disagree Nor Agree	Agree	Strongly Agree
		1	2	3	4	5
SE7:	Unauthorized employees are prohibited from accessing my organization's ePHI resources.	1 [ ]	2 [ ]	3 [ ]	4 [ ]	5 [ ]
SE8:	HIPAA security measures are implemented in my organization to prevent sensitive information from unauthorized disclosure.	1 [ ]	2 [ ]	3 [ ]	4 [ ]	5 [ ]
SE9:	My organization constantly updates ePHI resources and regularly creates information backups.	1 [ ]	2 [ ]	3 [ ]	4 [ ]	5 [ ]
SE10:	My organization regularly conducts risk assessment and updates HIPAA security plans to reduce the probability of loss of ePHI.	1 [ ]	2 [ ]	3 [ ]	4 [ ]	5 [ ]
SE11:	My organization has HIPAA security controls (such as change management procedures) in place to prevent unauthorized ePHI changes (creation, alternation, and deletion).	1 [ ]	2 [ ]	3 [ ]	4 [ ]	5 [ ]

Appendix B

IRB Approval

NOVA SOUTHEASTERN UNIVERSITY
Office of Grants and Contracts
Institutional Review Board

MEMORANDUM

To: James Brady

From: Ling Wang, Ph.D.
Institutional Review Board

Date: March 31, 2010

Re: *An Investigation of Factors that Affect HIPAA Security Compliance in Academic Medical Centers*

IRB Approval Number: wang03151006

I have reviewed the above-referenced research protocol at the center level. Based on the information provided, I have determined that this study is exempt from further IRB review. You may proceed with your study as described to the IRB. As principal investigator, you must adhere to the following requirements:

1) CONSENT: If recruitment procedures include consent forms these must be obtained in such a manner that they are clearly understood by the subjects and the process affords subjects the opportunity to ask questions, obtain detailed answers from those directly involved in the research, and have sufficient time to consider their participation after they have been provided this information. The subjects must be given a copy of the signed consent document, and a copy must be placed in a secure file separate from de-identified participant information. Record of informed consent must be retained for a minimum of three years from the conclusion of the study.

2) ADVERSE REACTIONS: The principal investigator is required to notify the IRB chair and me (954-262-5369 and 954-262-2020 respectively) of any adverse reactions or unanticipated events that may develop as a result of this study. Reactions or events may include, but are not limited to, injury, depression as a result of participation in the study, life-threatening situation, death, or loss of confidentiality/anonymity of subject. Approval may be withdrawn if the problem is serious.

3) AMENDMENTS: Any changes in the study (e.g., procedures, number or types of subjects, consent forms, investigators, etc.) must be approved by the IRB prior to implementation. Please be advised that changes in a study may require further review depending on the nature of the change. Please contact me with any questions regarding amendments or changes to your study.

The NSU IRB is in compliance with the requirements for the protection of human subjects prescribed in Part 46 of Title 45 of the Code of Federal Regulations (45 CFR 46) revised June 18, 1991.

Cc: Protocol File

3301 College Avenue • Fort Lauderdale, FL 33314-7796 • (954) 262-5369
Fax: (954) 262-3977 • Email: *inga@nsu.nova.edu* • Web site: www.nova.edu/cwis/ogc

Reference List

AAMC. (2007, September). *Consequences of heightened Department of Veterans Affairs information security on academic medical centers* [White paper]. Retrieved May 15, 2010, from http://www.aamc.org/members/gir/whitepaperonvasecurity.pdf

AAMC. (2009a). *About the AAMC.* Retrieved May 15, 2010, from http://www.aamc.org/about/start.htm

AAMC. (2009b). *GIR.* Retrieved May 15, 2010, from http://www.aamc.org/members/gir/start.htm

AAMC. (2009c). *Membership.* Retrieved May 15, 2010, from http://www.aamc.org/about/membership.htm

AAMC. (2009d). *HIPAA.* Retrieved May 15, 2010, from http://www.aamc.org/advocacy/hipaa/

Agarwal, R., & Karahanna, E. (2000). Time flies when you're having fun: Cognitive absorption and beliefs about information technology usage. *MIS Quarterly, 24*(4), 665-694.

Aguilar, M. K. (2009, May). Recovery act means big compliance challenges. *Compliance Week, 6*(64), 1-3.

Ajzen, I. (1985). From intentions to actions: A theory of planned behavior. In J. Kuhl & J. Beckmann (Eds.), *Action control: From cognition to behavior* (pp. 11-39). New York: Springer.

Ajzen, I. (1988). *Attitudes, personality, and behavior*. IL: Dorsey Press.

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes, 50*(2), 179-221.

Ajzen, I., & Fishbein, M. (1980). *Understanding attitudes and predicting social behavior*. Englewood Cliffs, NJ: Prentice-Hall.

Alison, P. A. (1998). *Multiple regression: A primer*. Thousand Oaks, CA: Pine Forge Press/Sage Publications.

Allen, D. K., & Fifield, N. (1999). Re-engineering change in higher education. *Information Research, 4*(3). Retrieved May 15, 2010, from http://informationr.net/ir/4-3/paper56.html

Alstete, J. (2006). Inside advice on educating managers for preventing employee theft. *International Journal of Retail & Distribution Management, 34*(11), 833-844.

Anderson, J. C., & Gerbing, D. W. (1992). Assumptions of the two-step approach to latent variable modeling. *Sociological Methods and Research, 20(*3), 321-333.

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

Baker, W. H., Hutton, A., Hylender, C. D., Novak, C., Porter, C., Sartin, B., et al. (2009). *2009 data breach investigations report* [White paper]. Retrieved May 15, 2010, from http://www.verizonbusiness.com/resources/security/reports/2009_databreach_rp.pdf

Bakhtiari, E. (2009). HITECH stiffens HIPAA requirements and penalties. *The Doctor's Office, 28*(7), 3-4.

Baldwin, A., Beres, Y., Shiu, S., & Kearney, P. (2006). A model-based approach to trust, security and assurance. *BT Technology Journal, 24*(4), 53-68.

Ball, D., & Levy, Y. (2008). Emerging educational technology: Assessing the factors that influence instructors' acceptance in information systems and other classrooms. *Journal of Information Systems Education, 19*(4), 431-443.

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

Bandura, A. (1986). *Social foundations of thought and action: A social cognitive theory.* Englewood Cliffs, NJ: Prentice Hall.

Bandura, A., & Wood, R. E. (1989). Effect of perceived controllability and performance standards on self-regulation of complex decision making. *Journal of Personality and Social Psychology, 56,* 805-814.

Barlas, S. (2009). Stimulus bill includes physician payments/penalties and HIPAA expansions. *Psychiatric Times, 26,* 34-35.

Barry, G., & Grossmeier, J. (2009). Is your incentive strategy sound? Guidelines for designing a HIPAA compliant wellness program. *Employee Benefit Plan Review, 64*(1), 5-8.

Beatson, J. G. (1991). Security—A personnel issue: The importance of personnel attitudes and security education. In K. Dittrich, S. Rautakivi & J. Saari (Eds.), *Computer Security and Information Integrity* (pp. 29-38). Amsterdam: Elsevier Science.

Bhatti, R., Moidu, K., & Ghafoor, A. (2006). Policy-based security management for federated healthcare databases (or RHIOs). *Proceedings of the International Workshop on Healthcare Information and Knowledge Management (HIKM '06),* 41-48.

Bia, M., & Kalika, M. (2007). Adopting an ICT code of conduct: An empirical study of organizational factors. *Journal of Enterprise Information Management, 20*(4), 432-446.

Bianchi, A. J. (2009). An overview of the impact of the American Recovery and Reinvestment Act of 2009 on the HIPAA medical privacy and security rules. *Tax Management Compensation Planning Journal, 37*(9), 227-236.

Blades, M. (2009). Stimulus bill tightens HIPAA privacy requirements. *Security Technology Executive, 19*(6), 36.

Blumstein, A., Cohen, J., & Nagin, D. (1978). *Deterrence and incapacitations: Estimating the effects of criminal sanctions on crime rates.* Washington, DC: National Academy of Sciences.

Boudreau, M., Gefen, D., & Straub, D. W. (2001). Validation in information systems research: A state-of-the-art assessment. *MIS Quarterly, 25*(1), 1-16.

Bowker, D. W., & Randerson, P. F. (2010). *Practical data analysis*. Harlow, Essex, UK: Pearson Education Limited.

Brenner, B. (2007, July). ISO 27001 could bridge the regulatory divide, expert says. *Information Security Magazine*. Retrieved May 15, 2010, from http://searchsecurity.techtarget.com/news/interview/0,289202,sid14_gci1263828,00.html#

Brown, B. (2009a). New technologies have created new threats to electronic protected health information. *Journal of Health Care Compliance, 11*(4), 35-38.

Brown, B. (2009b). Privacy provisions of the American Recovery and Reinvestment Act. *Journal of Health Care Compliance, 11*(3), 37-40.

Campbell, J. P., Dunnette, M. D., Lawler, E. E., III., & Weick, K., Jr. (1970). *Managerial behavior, performance and effectiveness*. New York: McGraw-Hill.

Carmines, E. G., & Zeller, R. A. (1991). *Reliability and viability assessment*. Thousand Oaks, CA: Sage.

Casmir, R., & Yngstrom, L. (2005). Towards a dynamic and adaptive information security awareness approach. *Proceedings of the IFIP TC11 WG11.8 4th World Conference on Information Security Education (WISE4),* Moscow, Russia, 162-173.

Cazier, J. A., Wilson, E. V., & Medlin, B. D. (2007). The role of privacy risk in IT acceptance: An empirical study. *International Journal of Information Security and Privacy, 1*(2), 61-66, 68-73.

Chan, M., Woon, I., & Kankanhalli, A. (2005). Perceptions of information security in the workplace: Linking information security climate to compliant behavior. *Journal of Information Privacy & Security, 1*(3), 18-41.

Chang, A. J., & Yeh, Q. (2006). On security preparations against possible IS threats across industries. *Information Management & Computer Security, 14*(4), 343-360.

Chang, S. E., & Ho, C. B. (2006). Organizational factors to the effectiveness of implementing information security management. *Industrial Management + Data Systems, 106*(3), 345-361.

Chang, S. E., & Lin, C. (2007). Exploring organizational culture for information security management. *Industrial Management + Data Systems, 107*(3), 438-458.

Chen, C. C., Shaw, R. S., & Yang, S. C. (2006). Mitigating information security risks by increasing user security awareness: A case study of an information security awareness system. *Information Technology, Learning, and Performance Journal, 24*(1), 1-14.

Chen, C. K., & Hughes, J. (2004). Using ordinal regression model to analyze student satisfaction questionnaires. *Association for Institutional Research, 1,* 1-21.

Chu, L. L. (2003). The effects of web page design instruction on computer self-efficacy of preservice teachers and correlates. *Journal of Educational Computing Research, 28*(2), 127-142.

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

Clarke, I., Flaherty, T. B., Hollis, S. M., & Tomallo, M. (2009). Consumer privacy issues associated with the use of electronic health records. *Academy of Health Care Management Journal, 5*(1/2), 63-77.

Cline, M., Guynes, C., & Nyanoga, A. (2010). The impact of organizational change on information systems security. *Journal of Business & Economics Research, 8*(1), 59-64.

CMS, Office of E-Health Standards and Services. (2008). *HIPAA compliance review analysis and summary of results.* Retrieved May 15, 2010, from http://www.cms.hhs.gov/Enforcement/Downloads/HIPAAComplianceReviewSumtopost508.pdf

Cohen, J. (1992). A power primer. *Psychological Bulletin, 112,* 155-159.

Collins, J. D. W. (2007). Toothless HIPAA: Searching for a private right of action to remedy privacy rule violations. *Vanderbilt Law Review*, *60*(1), 199-233.

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

Compeau, D. R., Higgins, C. A., & Huff, S. (1999). Social cognitive theory and individual reactions to computing technology: A longitudinal study. *MIS Quarterly, 23*(2), 145-158.

Conn, J. (2009). New sheriff in town. *Modern Healthcare, 39*(33), 13.

Connell, N. A. D., & Young, T. P. (2007). Evaluating healthcare information systems through an enterprise perspective. *Information & Management, 44*(4), 433-40.

Cooper, R. B. (2000). Information technology development creativity: A case study of attempted radical change. *MIS Quarterly*, *24*(2), 245-276.

Creswell, J. W. (2005). *Educational research: Planning, conducting, and evaluating quantitative and qualitative research* (2nd ed.). Upper Saddle River, NJ: Pearson.

Curry, A., & Moore, C. (2003). Assessing information culture: An exploratory model. *International Journal of Information Management, 23*(2), 91-110.

D'Arcy, J. & Hovav, A. (2009). Does one size fit all? Examining the differential effects of IS security countermeasures. *Journal of Business Ethics, 89*, 59-71.

DataLossDB. (2010). *Incidents.* Retrieved May 15, 2010, from http://datalossdb.org/search?direction=desc&order=reported_date&org_type[]=Med

Da Veiga, A., & Eloff, J. H. P. (2007). An information security governance framework. *Information Systems Management, 24*(4), 361-372.

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

Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1989). User acceptance of computer technology: A comparison of two theoretical models. *Management Science, 35*(8), 982-1003.

Davis, J. W. (2009). HITECH HIPAA amendments: New rules on breach notification, business associate compliance, and enforcement. *The Health Lawyer, 21*(5), 23-29.

Deal, T., & Kennedy, A. (1982). *Corporate culture: The rites and rituals of corporate life*. New York: Addison-Wesley.

DeVellis, R. F. (2003). *Scale development. Theory and applications* (2nd ed.). Thousand Oaks, CA: Sage.

Dhillon, G. (2001). Challenges in managing information security in the new millennium. In G. Dhillon (Ed.), *Information security management* (pp. 1-9). Hershey, PA: Idea Group.

Dhillon, G., & Backhouse, J. (2001). Current directions in IS security research: Towards socio-organizational perspectives. *Information Systems Journal, 11*(2), 127-153.

Dillon, A., & Morris, G. M. (1996). User acceptance of information technology: Theories and models. In M. Williams (Eds.), *Annual review of information science and technology* (Vol. 31, pp. 3-32). Medford, NJ: Information Today.

Dimitropoulos, L., & Rizk, S. (2009). A state-based approach to privacy and security for interoperable health information exchange. *Health Affairs, 28*(2), 428-434.

Dinev, T., & Hart, P. (2006). Internet privacy concerns and social awareness as determinants of intentional to transact. *International Journal of Electronic Commerce, 10*(2), 7-29.

Dinev, T., & Hu, Q. (2007). The centrality of awareness in the formation of user behavioral intention toward protective information technologies. *Journal of the Association for Information Systems, 8*(7), 386-392, 394-408.

Dowell, M. (2009). HHS and FTC release guidance on HITECH act requirements. *Journal of Health Care Compliance, 11*(4), 5-10.

Drew, M. (2007). Information risk management and compliance: Expect the unexpected. *BT Technology Journal, 25*(1), 19-29.

Drumke, M. W. (2008). A HIPAA primer. *The Brief, 37*(3), 34-43.

Ehrlich, L. (1973). Participation in illegitimate activities: A theoretical and empirical investigation. *Journal of Political Economy, 81,* 521-564.

Ellis, T. J., & Levy, Y. (2008). A framework of problem-based research: A guide for novice researchers on the development of a research-worthy problem. *Informing Science Journal, 11,* 17-33.

Ellis, T. J., & Levy, Y. (2009). Towards a guide for novice researchers on research methodology: Review and proposed methods. *Issues in Informing Science and Information Technology, 6,* 323-337.

Ernst & Young. (2009). *The 2009 Ernst & Young business risk report: The top 10 risks in global business* [White paper]. Retrieved May 15, 2010, from http://www.ey.com/Publication/vwLUAssets/2009_business_risk_report/$FILE/2009_business_risk_report.pdf

Filipek, R. (2007). European nations make security a high priority. *The Internal Auditor, 64*(5), 8, 15-16.

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

Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research, 18*(1), 39-50.

Fritsche, G. D., & Rodgers, S. K. (2007). Encryption technologies: Testing and identifying campus needs. *Proceedings of the 35th Annual ACM SIGUCCS Conference on User Services (SIGUCCS '07)*, 109-112.

Frost & Sullivan. (2008). *The 2008 (ISC)^2 global information security workforce study* [White paper]. Retrieved May 15, 2010, from http://www.isc2.org/uploadedFiles/Industry_Resources/2008_Global_WF_Study.pdf

Gable, J. (2005, July/August). Navigating the compliance landscape. *The Information Management Journal*, *39*(4), 1-6.

Gallagher, L. (2009). *2009 HIMSS security survey: Statement to the HIT Standards Committee Privacy and Security Workgroup* [Testimony]. Retrieved May 15, 2010, from http://healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_11673_909260_0_0_18/GallagherHIMSSTestimony.pdf

Glaser, B. G., & Strauss, A. L. (1967). *The discovery of grounded theory: Strategies for qualitative research*. New York: Aldine.

Goodhue, D. L., & Straub, D. W. (1989). Security concerns of system users: A proposed study of user perceptions of the adequacy of security measures. *Twenty-Second Annual Hawaii International Conference on System Science (HICSS)*, Kailua-Kona, HI.

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

Greenberg, M. D., & Ridgely, M. S. (2009). Crossed wires: How yesterday's privacy rules might undercut tomorrow's nationwide health information network. *Health Affairs*, *28*(2), 450-452.

Griffin, M. A., & Neal, A. (2000). Perceptions of safety at work: A framework for linking safety climate to safety performance, knowledge and motivation. *Journal of Occupational Health Psychology, 5*(3), 347-358.

Gross, J. B., & Rosson, M. B. (2007). Looking for trouble: Understanding end-user security management. *Proceedings of the 2007 Symposium on Computer Human interaction For the Management of information Technology (CHIMIT '07)*, 1-10.

Gupta, A., & Hammond, R. (2005). Information systems security issues and decisions for small businesses: An empirical examination. *Information Management & Computer Security, 13*(4), 297-310.

Guzman, I. R., Stam, K. R., & Stanton, J. M. (2008). The occupational culture of IS/IT personnel within organizations. *SIGMIS Database, 39*(1), 33-50.

Hair, J., Anderson, R., Tatham, R., & Black, W. (1984). *Multivariate data analysis.* Upper Saddle River, NJ: Prentice Hall.

Hale, J., & Brusil, P. (2007). Secur(e/ity) management: A continuing uphill climb. *Journal of Network and Systems Management, 15*(4), 525-553.

Happ, J. (2006). Eight steps to integrating security standards. *Biomedical Instrumentation & Technology*, 22-24.

Hasemyer, D. (2009, July 17). Hotline for UCSD patients swamped. *San Diego Union-Tribune*. Retrieved May 15, 2010, from http://www3.signonsandiego.com/stories/2009/jul/17/1m17hacker221630-hotline-ucsd-patients-swamped/?technology&zIndex=133482

Havelka, D. (2003). Predicting software self-efficacy among business students: A preliminary assessment. *Journal of Information Systems Education, 14*(2), 145-152.

Hawkey, K., Muldner, K., & Beznosov, K. (2008). Searching for the right fit: Balancing IT security management model trade-offs. *IEEE Internet Computing, 12*(3), 22-30.

Hayes, B. E., Perander, J., Smecko, T., & Trask, J. (1998). Measuring perceptions of workplace safety: Development and validation of work safety scale. *Journal of Safety Research, 29*(3), 145-161.

Hazari, S. (2005). Perceptions of end-users on the requirements in personal firewall software: An exploratory study. *Journal of Organizational and End User Computing, 17*(3), 47-65.

Hazari, S., Hargrave, W., & Clenney, B. (2008). An empirical investigation of factors influencing information security behavior. *Journal of Information Privacy & Security, 4*(4), 3-20.

Helms, M. M., Moore, R., & Ahmadi, M. (2008). Information technology (IT) and the healthcare industry: A SWOT analysis. *International Journal of Healthcare Information Systems and Informatics, 3*(1), 75-92.

Herold, R. (2009a, March 23). HIPAA enforcement, more government audits leading to more convictions. *Search Compliance.* Retrieved May 15, 2010, from http://searchcompliance.techtarget.com/tip/0,289483,sid195_gci1351650_mem1,00.html?track=NL-1168&ad=698061&Offer=sCOunsc040209h&asrc=EM_USC_6494269

Herold, R. (2009b, March 23). HIPAA enforcement getting stronger. *Search Compliance.* Retrieved May 15, 2010, from http://searchcompliance.techtarget.com/tip/0,289483,sid195_gci1351601_mem1,00.html

HHS guidance on securing protected health information and avoiding breach notification. (2009). *Medical Benefits, 26*(13), 7-8.

Hill, T., & Lewicki, P. (2006). *Statistics: Methods and applications*. Tulsa: StatSoft, Inc.

HIPAA. (1996). Pub. L. No. 104-191, 110 Stat. 1936.

HIPAA. (2005a). 45 CFR § 160.103.

HIPAA. (2005b). 45 CFR § 160.203.

HIPAA. (2005c). 45 CFR § 160.404.

HIPAA. (2005d). 45 CFR § 164.304.

HIPAA. (2005e). 45 CFR § 164.306(a).

HIPAA violation costs CVS $2.25 million. (2009). *Information Management Journal, 43*(3), 15.

Hisham, M. B. (2008). *Detecting outliers.* Retrieved May 15, 2010, from http://www.hishammb.net/workshopfeb2008/outlierinspss.pdf

Hoffmann, J. P. (2004). *Generalized linear models: An applied approach.* Boston: Pearson Education Inc.

Hoffman, S., & Podgurski, A. (2007). Securing the HIPAA Security Rule. *Journal of Internet Law, 6*(26), 1-18.

Holland, E. S. (2009). *HIPAA security compliance reviews.* Retrieved May 15, 2010, from http://csrc.nist.gov/news_events/HIPAA-May2009_workshop/presentations/2-051809-cms-security-compliance-reviews.pdf

Holloway, M. (2009). HITECH: HIPAA gets a facelift. *Benefits Law Journal, 22*(3), 85-89.

Hong, K., Chi, Y., Chao, L. R., & Tang, J. (2006). An empirical study of information security policy on information security elevation in Taiwan. *Information Management & Computer Security, 14*(2), 104-115.

Hourihan, C. (2009, May 25). *Recap: A CMS & NIST HIPAA Security Rule conference.* Message posted to https://www.hitrustcentral.net/blogs/ht/archive/2009/05/25/recap-a-cms-amp-nist-HIPAA-security-rule-conference.aspx

Huang, L., Bai, X., & Nair, S. (2008). Developing a SSE-CMM-based security risk assessment process for patient-centered healthcare systems. *Proceedings of the 6th International Workshop on Software Quality (WoSQ '08),* Leipzig, Germany, 11-16.

Huebner, R. A., & Britt, M. M. (2006). Analyzing enterprise security using social networks and structuration theory. *Journal of Applied Management and Entrepreneurship, 11*(3), 68-77.

Im, G. P., & Baskerville, R. L. (2005). A longitudinal study of information system threat categories: The enduring problem of human error. *The Data Base for Advances in Information Systems, 36*(4), 68-79.

Jackson, J. H., & Adams, S. W. (1979). The life cycle of rules. *The Academy of Management Review, 4*(2), 269-273.

Jahankhani, H., Fernando, S., Nkhoma, M. Z., & Mouratidis, H. (2007). Information systems security: Cases of network administrator threats. *International Journal of Information Security and Privacy, 1*(3), 13-25.

Jahankhani, H., & Nkhoma, M. Z. (2005). Information systems risk assessment. *International Conference on Information and Communication Technology in Management (ICTM),* Malaysia, 426-437.

James, P. N. (1992). Education and training. *Information Systems Management, 9*(2), 15-21.

Jarrell, K., Welker, J., Silsbee, D., & Tucker, F. (2008). The unintended effects of the HIPAA privacy protections on health care treatment team and patient outcomes. *The Business Review, 11*(1), 14-25.

Jennex, M. E. (2007). Knowledge management and security: A call for research. *International Journal of Knowledge Management, 3*(1), i-iv.

Jerbic, M. (2008). Today's imperative is information-centric security. *DM Review, 18*(5), 18.

Johnston, A. C., & Warkentin, M. (2008). Information privacy compliance in the healthcare industry. *Information Management & Computer Security, 16*(1), 5-19.

Joreskog, K. G., & Sorbom, D. (1996). *LISREL 8: Structural equation modeling*. Chicago: Scientific Software International Corp.

Kalakota, R., & Whinston, A. (1997). *Electronic commerce: A manager's guide*. Reading, MA: Addison Wesley.

Kamal, M. (2008). The psychology of IT security in business. *Journal of American Academy of Business, 13*(1), 145-150.

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

Kaplowitz, D. M., Hadlock, D. T., & Levine, R. (2004). A comparison of web and mail survey response rates. *Public Opinion Quarterly, 68*, 94-101.

Karyda, M., Mitrou, E., & Quirchmayr, G. (2006). A framework for outsourcing IS/IT security services. *Information Management & Computer Security, 14*(5), 402-415.

Keith, M., Shao, B., & Steinbart, P. (2009). A behavioral analysis of passphrase design and effectiveness. *Journal of the Association for Information Systems, 10*(2), 63-89.

Kennerley, M., & Neely, A. (2002). A framework of factors affecting the evolution of performance measurement systems. *International Journal of Operations & Production Management, 22*(11), 1222-1245.

Kerlinger, F. N., & Lee, H. B. (2000). *Foundations of behavioral research* (4th ed.). Holt, NY: Harcourt College.

Kim, E. B. (2005). Information security awareness status of full time employees. *The Business Review, 3*(2), 219-226.

Kim, J. O. (1975). Multivariate analysis of ordinal variables. *American Journal of Sociology, 81*, 261-298.

Kim, M., & Ahn, J. (2007). Management of in the e-marketplace: The role of the buyer's experience in building trust. *Journal of Information Technology, 22*(2), 119-132.

King, W. R., & He, J. (2005). External validity in IS survey research. *Communications of the Association for Information Systems, 16*, 880-894.

Kirkpatrick, J. (2006). Protect your business against dangerous information leaks. *Machine Design, 78*(3), 66.

Kitchenham, A. B., & Pfleeger, L. S. (2002). Principles of survey research: Part 3: Constructing a survey instrument. *ACM SIGSOFT Software Engineering Notes, 27*(2), 20-24.

Klete, H. (1975). Some minimum requirements for legal sanctioning systems with special emphasis on detection. In A. Blumstein, J. Cohen, & D. Nagin (Eds.), *Deterrence and incapacitation: Estimating the effects of criminal sanctions on crime rates.* Washington, DC: National Academy of Sciences.

Knapp, K. J., & Boulton, W. R. (2006). Cyber-warfare threatens corporations: Expansion into commercial environments. *Information Systems Management, 23*(2), 76-87.

Knapp, K. J., Marshall, T. E., Rainer, R. K., & Ford, F. N. (2006). Information security: Management's effect on culture and policy. *Information Management & Computer Security, 14*(1), 24-36.

Knapp, K. J., Marshall, T. E., Rainer, R. K., Jr., & Ford, F. N. (2007). Information security effectiveness: Conceptualization and validation of a theory. *International Journal of Information Security and Privacy, 1*(2), 37-40, 42-47, 51-60.

Komarek, R. P., & Moore, W. A. (2004). Fast robust logistic regression for large spare datasets with binary outputs. *British Ecological Society Journal of Ecology, 92,* 372-383.

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

Kruck, S. E., & Teer, F. P. (2008). Computer security practices and perceptions of the next generation of corporate computer users. *International Journal of Information Security and Privacy, 2*(1), 80-90.

Lallmahamood, M. (2007). An examination of individual's perceived security and privacy of the Internet in Malaysia and the influence of this on their intention to use e-commerce: Using an extension of the technology acceptance model. *Journal of Internet Banking and Commerce, 12*(3), 1-26.

Langford, M., & Reeves, T. E. (1998). The relationships between computer self-efficacy and personal characteristics of the beginning information systems student. *Journal of Computer Information Systems , 38*(4), 41-45.

Lawrence, S. C. (2007). Access anxiety: HIPAA and historical research. *Journal of the History of Medicine and Allied Sciences, 62*(4), 422-460.

Leach, J. (2003). Improving user security behavior. *Computers and Security, 22*(8), 685-692.

Leedy, P. D., & Ormrod, J. E. (2005). *Practical research: Planning and design* (8th ed.). Upper Saddle River, NJ: Prentice Hall.

Leidner, D. E., & Jarvenpaa, S. L. (1995). The use of information technology to enhance management school education: A theoretical view. *MIS Quarterly, 19*(3), 265-291.

Leidner, D. E., & Kayworth, T. (2006). A review of culture in information systems research: Towards a theory of IT-culture conflict. *MIS Quarterly, 30*(2), 357-399.

Lending, D., & Dillon, T. W. (2007). The effects of confidentiality on nursing self-efficacy with information systems. *International Journal of Healthcare Information Systems and Informatics, 2*(3), 49-54, 56-64.

Levy, Y. (2006). *Assessing the value of e-learning systems*. Hershey, PA: Information Science.

Levy, Y., & Green, B. D. (2009). An empirical study of computer self-efficacy and the technology acceptance model in the military: A case of a U.S. Navy combat information system. *Journal of Organizational and End User Computing, 21*(3), 1-23.

Lewis, R. B., Templeton, F. G., & Byrd, T. A. (2005). A methodology for construct development in MIS research. *European Journal of Information Systems, 14*, 388-400.

Li, J., & Shaw, M. J. (2008). Electronic medical records, HIPAA, and patient privacy. *International Journal of Information Security and Privacy*, *2*(3), 45-54.

Lin, H. (2007). Knowledge sharing and firm innovation capability: An empirical study. *International Journal of Manpower*, *28*(3/4), 315-332.

Lineberry, S. (2007). The human element: The weakest link in information security. *Journal of Accountancy, 204*(5), 44-46, 49.

Loch, K. D., Straub, D. W., & Kamel, S. (2003). Diffusing the Internet in the Arab world: The role of social norms and technological culturation. *IEEE Transactions on Engineering Management, 50*(1), 45-64.

Logan, P. Y., & Noles, D. (2008). Protecting patient information in outsourced telehealth services: Bolting on security when it cannot be baked in. *International Journal of Information Security and Privacy*, *2*(3), 55-70.

Loghry, J. D., & Veach, C. B. (2009). Enterprise risk assessments: Holistic approach provides companywide perspective. *Professional Safety, 54*(2), 31-35.

Ma, Q., Johnston, A. C., & Pearson, J. M. (2008). Information security management objectives and practices: A parsimonious framework. *Information Management & Computer Security, 16*(3), 251-270.

Madnick, E. S. (1978, Fall). Management policies and procedures needed for effective computer security. *Sloan Management Review*, 61-74.

Maffeo, M. (2009). The relationship of privacy provisions in the stimulus bill to health information technology. *Journal of Health Care Compliance, 11*(3), 55-58.

Magklaras, G. B., Furnell, S. M., & Brooke, P. J. (2006). Towards an insider threat prediction specification language. *Information Management & Computer Security 14*(4), 361-381.

Martin, J. (1973). *Security, accuracy, and privacy in computer systems*. Englewood Cliffs, NJ: Prentice-Hall.

McFadzean, E., Ezingeard, J., & Birchall, D. (2007). Perception of risk and the strategic impact of existing IT on information security strategy at board level. *Online Information Review, 31*(5), 622.

McGraw, D., Dempsey, J. X., Harris, L., & Goldman, J. (2009). Privacy as an enabler, not an impediment: Building trust into health information exchange. *Health Affairs, 28*(2), 416-427.

Medlin, B. D., & Cazier, J. A. (2007). An empirical investigation: Health care employee passwords and their crack times in relationship to HIPAA security standards. *International Journal of Healthcare Information Systems and Informatics, 2*(3), 39-48.

Medlin, B. D., Cazier, J. A., & Foulk, D. P. (2008). Analyzing the vulnerability of U.S. hospitals to social engineering attacks: How many of your employees would share their password? *International Journal of Information Security and Privacy, 2*(3), 71-83.

Mertler, C. A., & Vannatta, R. A. (2001). *Advanced and multivariate statistical methods: Practical application and interpretation*. Los Angeles: Pyrczak.

Mills, J., Platts, K., & Gregory, M. (1995). A framework for design of manufacturing strategy processes: A contingency approach. *International Journal of Operations and Production Management, 15*(4), 17-49.

Mitnick, K. (2003). Are you the weak link? *Harvard Business Review, 81*(4), 18-20.

Moreira, E. D. S., Martimiano, L. A. F., Brandão, A. J. D. S, & Bernardes, M. C. (2008). Ontologies for information security management and governance. *Information Management & Computer Security, 16*(2), 150-165.

Moynihan, J. F. (2007). Confronting the emerging threat. *The Internal Auditor, 64*(5), 66-70.

Myler, E., & Broadbent, G. (2006). ISO 17799: Standard for security. *Information Management Journal*, *40*(6), 43-44, 46, 48-52.

Nash, K. (2008, October). The global state of information security 2008. *CSO Magazine*. Retrieved May 15, 2010, from http://www.csoonline.com/article/454939/The_Global_State_of_Information_Security

Neal, A., & Griffin, M. A. (1997). Perceptions of safety at work: Developing a model to link organizational safety climate and individual behavior. *Proceedings of the 12th Annual Conference of the Society for Industrial and Organizational Psychology,* St. Louis, MO.

Neufeld, D. J., Dong, L., & Higgins, C. (2007). Charismatic leadership and user acceptance of information technology. *European Journal of Information Systems*, *16*(4), 494-510.

North, M. M., North, M. M., & North, S. M. (2009). Security from the bottom-up: Compliance regulations and the trend toward design-oriented web applications. *Journal of Computing Sciences in Colleges*, *24*(4), 54-60.

Novakovic, L., McGill, T., & Dixon, M. (2009). Understanding user behavior towards passwords through acceptance and use modelling. *International Journal of Information Security and Privacy*, *3*(1), 11-29.

NSU Libraries. (n.d.). Retrieved May 15, 2010, from https://novacat.nova.edu/validate?url=http%3A%2F%2F0-elib.nova.edu.novacat.nova.edu%3A80%2Fdb%2Fn%2Fnsearch.cfm

O'Brien, R. M. (2007). A caution regarding rules of thumb for variance inflation factors. *Quality and Quantity*, 41, 673-690.

Organization for Economic Cooperation and Development. (2002). *OECD guidelines for the security of information systems and networks: Toward a culture of security.* Retrieved May 15, 2010, from http://www.oecd.org/dataoecd/16/22/15582260.pdf

Palvia, P., Leary, T., Mao, E., Midha, P., Pinjani, P., & Salam, A. F. (2004). Research methodologies in MIS: An update. *Communications of the AIS, 14*, 526-542.

Pattinson, M. R., & Anderson, G. (2007). How well are information risks being communicated to your computer end-users? *Information Management & Computer Security*, *15*(5), 362-371.

Pavlou, P. A., & Fygenson, M. (2006). Understanding and predicting electronic commerce adoption: An extension of the theory of planned behavior. *MIS Quarterly*, *30*(1), 115-143.

Payton, A. M. (2006). Data security breach: Seeking a prescription for adequate remedy. *Proceedings of the 3rd annual conference on Information security curriculum development (InfoSecCD '06),* 162-167.

Peters, S. (2009). *The 14th annual CSI computer crime and security survey: Executive summary* [White paper]. Retrieved May 15, 2010, from http://www.hlncc.com/docs/CSI_Survey_2009_Executive_Summary.pdf

Pfleeger, S. L., & Rue, R. (2008). Cybersecurity economic issues: Clearing the path to good practice. *IEEE Software, 25*(1), 35.

Pinsonneault, A., & Kraemer, K. (1993). Survey research methodology in management information systems: An assessment. *Journal of Management Information Systems 10*(2), 75-105.

Pirim, T., James, T., Boswell, K., Reithel, B., & Barkhi, R. (2008). An empirical investigation of an individual's perceived need for privacy and security. *International Journal of Information Security and Privacy, 2*(1), 42-53.

Ponemon, L. P. (2008). 2009 security mega trends survey. *Ponemon Institute LLC.* [White paper]. Retrieved May 15, 2010, from http://www.lumension.com/viewDocument.jsp?id=148524

Porter, S., & Whitcomb, E. M. (2003). The impact of contact type on web survey response rate. *Public Opinion Quarterly, 67,* 579-588.

Privacy Rights Clearinghouse. (2010). *A chronology of data breaches.* Retrieved May 15, 2010, from http://www.privacyrights.org/ar/ChronDataBreaches.htm#CP

Pumphrey, L. D., Trimmer, K., & Beachboard, J. (2007). Enterprise resource planning systems and HIPAA compliance. *Research in Healthcare Financial Management, 11*(1), 57-75.

Ramanathan, J., Cohen, R. J., Plassmann, E., & Ramamoorthy, K. (2007). Role of an auditing and reporting service in compliance management. *IBM Systems Journal, 46*(2), 305-318.

Rath, K. (2009). Health care information goes HITECH. *Collector, 75*(1), 22-25.

Reichers, A. E., & Schneider, B. (1990). *Organizational climate and culture: Evolution of constructs, organizational climate and culture*. B. Schneider (Ed.), *Title of book.* San Francisco: Jossey-Bass.

Rennie, L., & Shore, M. (2007). An advanced model of hacking. *Security Journal, 20*(4), 236-251.

Responsible information management: Ensuring data privacy in the enterprise. (2009). *OpRisk & Compliance*, 4-5.

Rhoades, L., & Eisenberger, R. (2002). Perceived organizational support: A review of the literature. *Journal of Applied Psychology, 87*(4), 698-714.

Rhodes, S. D., Bowie, A. D., & Hergenrather, C. K. (2003). Collecting behavioral data using the world wide web: Considerations for researchers. *Journal of Epidemiology and Community Health, 57*, 68-73.

Rifon, N. J., LaRose, R., & Choi, S. M. (2005). Your privacy is sealed: Effects of Web privacy seals on trust and personal disclosures. *The Journal of Consumer Affairs, 39*(2), 339-364.

Rogers, E. M. (1962). *Diffusion of innovation*. New York: Free Press.

Ross, W. H., & Chen, J. V. (2007). Labor arbitrators consider HIPAA: Guidance for health care managers. *Labor Law Journal, 58*(2), 117-130.

Rotvold, G. (2008). How to create a security culture in your organization. *Information Management Journal, 42*(6), 32-34, 36-38.

Ruighaver, A. B., & Maynard, S. (2006). Organizational security culture: More than just an end-user phenomenon. *Proceedings of the 21st IFIP TC-11 International Information Security Conference (IFIP/SEC '06),* Karlstad, Sweden, 425-430.

Ruzic, K. (2009). The next evolution of HIPAA security. *Journal of Health Care Compliance, 11*(3), 23-28.

Schein, E. H. (1992). *Organizational culture and leadership.* San Francisco: Jossey-Bass.

Schein, E. H. (1999). *The corporate culture survival guide*. San Francisco: Jossey-Bass.

Schmidt, M. B., Johnston, A. C., Arnett, K. P., Chen, J. Q., & Li, S. (2008). A cross-cultural comparison of U.S. and Chinese computer security awareness. *Journal of Global Information Management, 16*(2), 91-103.

Schnake, M. E. (1983). An empirical assessment of the effects of affective response in the measurement of organizational climate. *Personnel Psychology, 36*(4), 791-807.

Schulman, R. (2006). HIPAA privacy and security implications for field triage. *Prehospital Emergency Care, 10*(3), 340-342.

Sekaran, U. (2003). *Research methods for business: A skill building approach* (4th ed.). Hoboken, NJ: John Wiley & Sons.

Shevade, K. S., & Keerthi, S. S. (2003). A simple and efficient algorithm for gene selection using sparse logistic regression. *Oxford University Press, 19*(17), 2246-2253.

Siponen, M. T. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security, 8*(1), 31-41.

Siponen, M. T. (2001). An analysis of the recent IS security development approaches: Descriptive and prescriptive implications. In G. Dhillon (Ed.), *Information security management: Global challenges in the new millennium*, Hershey, PA: Idea Group.

Smith, S., & Jamieson, R. (2006). Determining key factors in e-government information systems security. *Information Systems Management, 23*(2), 23-32.

Social Security Act. (2005a). 42 USC § 1320d.

Social Security Act. (2005b). 42 USC § 1320d-5.

Sprinthall, R. (1997). *Basic statistical analysis*. Boston: Allyn and Bacon.SPSS. (n.d.). *PASW statistics.* Retrieved May 15, 2010, from http://www.spss.com/statistics/

Steinbrook, R. (2009). Health care and the American Recovery and Reinvestment Act. *The New England Journal of Medicine, 360*(11), 1057-60.

Straub, D. W. (1989). Validating instruments in MIS research. *MIS Quarterly, 13*(2), 147-170.

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

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

Strauss, A., & Corbin, J. (1998). *Basics of qualitative research. Techniques and procedures for developing grounded theory* (2nd ed.). Thousand Oaks, CA: Sage.

Sun, F., Omachi, S., Kato, N., Aso, H., Kono, S., & Takagi, T. (2000). Two-stage computational cost reduction algorithm based on Mahalanobis distance approximations. *Proceedings of the 15th International Conference on Pattern Recognition (ICPR'00), 2,* 2696.

Sun, H., & Zhang, P. (2006). The role of moderating factors in user technology acceptance. *International Journal of Human-Computer Studies, 64*(2), 53-78.

SurveyMonkey® (n.d.). *The simple way to create surveys.* Retrieved May 15, 2010, from http://www.surveymonkey.com/Default.aspx

Sveen, F. O., Rich, E., & Jager, M. (2007). Overcoming organizational challenges to secure knowledge management. *Information Systems Frontiers, 9*(5), 481-492.

Swartz, N. (2006). HIPAA compliance declines, survey says. *Information Management Journal, 40*(4), 16.

Swearingen, M. J. (2009). Penalties for health privacy violations increase. *HR Magazine, 54*(6), 30.

Tabachnick, B. G., & Fidell, L. S. (2007). *Using multivariate statistics*. Boston: Allyn and Bacon.

Tan, H. H., & Zhao, B. (2003). Individual- and perceived contextual-level antecedents of individual technical information inquiry in organizations. *The Journal of Psychology, 137*(6), 597-621.

Tang, J. (2008). The implementation of Deming's system model to improve security management: A case study. *International Journal of Management, 25*(1), 54-68, 198.

Taylor, R. B. (2006). *Academic medicine: A guide for clinicians* (1st ed.). New York: Springer Science+Business Media.

Taylor, S., & Todd, P. (1995). Understanding information technology usage: A test of competing models. *Information Systems, 6*(2), 144-176.

Teer, F. P., Kruck, S. E., & Kruck, G. P. (2007). Empirical study of students' computer security practices/perceptions. *The Journal of Computer Information Systems, 47*(3), 105-110.

Thielst, C. B. (2007). The future of healthcare technology. *Journal of Healthcare Management, 52*(1), 7-9.

Thomas, G., & Botha, R. A. (2007). Secure mobile device use in healthcare guidance from HIPAA and ISO17799. *Information Systems Management, 24*(4), 333-342.

Thompson, R. L., Higgins, C. A., & Howell, J. M. (1994). Influence of experience on personal computer utilization: Testing a conceptual model. *Journal of Management Information Systems, 11*(1), 167-188.

Thomson, M. E., & von Solms, R. (1998). Information security awareness: Educating your users effectively. *Information Management & Computer Security, 6*(4), 167-173.

Touchet, B. K., Drummond, S. R., & Yates, W. R. (2004). The impact of fear of HIPAA violation on patient care. *Psychiatric Services, 55*(5), 575-576.

Tsohou, A., Kokolakis, S., Karyda, M., & Kiountouzis, E. (2008). Process-variance models in information security awareness research. *Information Management & Computer Security, 16*(3), 271-287.

Vallerand, R. J. (1997). Toward a hierarchical model of intrinsic and extrinsic motivation. In M. P. Zanna (Ed.), *Advances in experimental social psychology* (Vol. 29, pp. 271-360). New York: Academic Press.

Venkatesh, V., & Davis, F. (1996). A model of the antecedents of perceived ease of use: Development and test. *Decision Science, 27*(3), 451-481.

Venkatesh, V., & Davis, F. (2000). A theoretical extension of the technology acceptance model: Four longitudinal field studies. *Management Science, 46*(2), 186-204.

Venkatesh, V., Morris, M. G., Davis, B. G., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly, 27*(3), 425-454.

Volonino, L., & Robinson, S. R. (2004). *Principles and practice of information security: Protecting computers from hackers and lawyers*. Upper Saddle River, NJ: Pearson Prentice Hall.

Von Solms, B. (2000). Information security: The third wave? *Computers and Security, 19*(7), 615-620.

Wade, J. (2004). The weak link in IT security. *Risk Management, 51*(7), 32-37.

Walters, L. M. (2007). A draft of an information systems security and control course. *Journal of Information Systems, 21*(1), 123-148.

White, G. L., Shah, J. R., Cook, J. R., & Mendez, F. (2008). Relationship between information privacy concerns and computer self-efficacy. *International Journal of Technology and Human Interaction, 4*(2), 52-62, 64-68, 70-82.

Wicke, S. (2003). Training the troops for HIPAA compliance: Are you ready? *Journal of Health Compliance, 5*(2), 41-42.

Williams, P. (2008). A practical application of CMM to medical security capability. *Information Management & Computer Security, 16*(1), 58-73.

Winkel, O. (2001). Multilateral security: A question of social organization and culture. In H. Böll-Stiftung (Ed.), *Arms control in cyberspace* (pp. 54-56), Berlin.

Winkel, O. (2007). Electronic government and network security: A viewpoint. *Transforming Government: People, Process and Policy, 1*(3), 220-229.

Womble, J. (2008). E-learning: The relationship among learner satisfaction, self-efficacy, and usefulness. *The Business Review, 10*(1), 182-188.

Worries over corporate reputation making information security a top priority. (2008). *International Journal of Micrographics & Optical Technology, 26*(1/2), 7-8.

Wyne, M. F., & Haider, S. N. (2007). HIPAA compliant HIS in J2EE environment. *International Journal of Healthcare Information Systems and Informatics, 2*(4), 73-89.