



5-2007

Status of Security Awareness In Business Organizations And Colleges of Business: An Analyses Of Training And Education, Policies, And Social Engineering Testing

Glenda M. Rotvold

Follow this and additional works at: <https://commons.und.edu/theses>

 Part of the [Psychology Commons](#)

Recommended Citation

Rotvold, Glenda M., "Status of Security Awareness In Business Organizations And Colleges of Business: An Analyses Of Training And Education, Policies, And Social Engineering Testing" (2007). *Theses and Dissertations*. 722.
<https://commons.und.edu/theses/722>

This Dissertation is brought to you for free and open access by the Theses, Dissertations, and Senior Projects at UND Scholarly Commons. It has been accepted for inclusion in Theses and Dissertations by an authorized administrator of UND Scholarly Commons. For more information, please contact zeinebyousif@library.und.edu.

STATUS OF SECURITY AWARENESS IN BUSINESS ORGANIZATIONS
AND COLLEGES OF BUSINESS: AN ANALYSIS OF
TRAINING AND EDUCATION, POLICIES,
AND SOCIAL ENGINEERING TESTING

by

Glenda M. Rotvold
Bachelor of Arts, Concordia College, 1974
Master of Science, University of North Dakota, 1992

A Dissertation

Submitted to the Graduate Faculty

of the

University of North Dakota

in partial fulfillment of the requirements

for the degree of

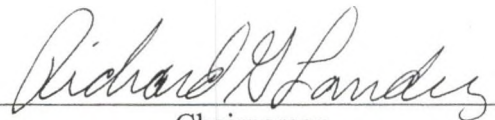
Doctor of Philosophy

Grand Forks, North Dakota

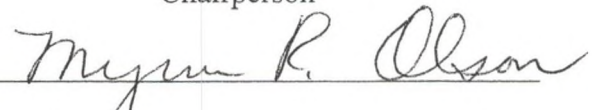
May
2007

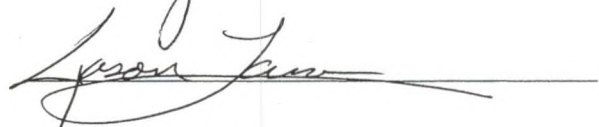
Copyright 2007 Glenda M. Rotvold

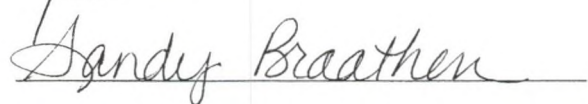
This dissertation, submitted by Glenda M. Rotvold in partial fulfillment of the requirements for the Degree of Doctor of Philosophy from the University of North Dakota, has been read by the Faculty Advisory Committee under whom the work has been done and is hereby approved.



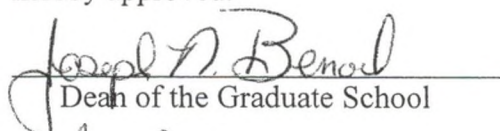
Chairperson

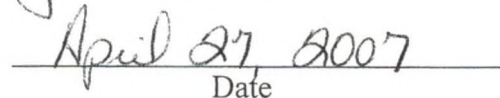






This dissertation meets the standards for appearance, conforms to the style and format requirements of the Graduate School of the University of North Dakota, and is hereby approved.


Dean of the Graduate School


Date

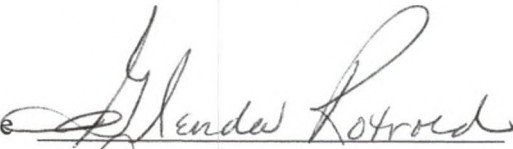
PERMISSION

Title Status of Security Awareness in Business Organizations and Colleges of
Business: An Analysis of Training and Education, Policies, and Social
Engineering Testing

Department Teaching and Learning

Degree Doctor of Philosophy

In presenting this dissertation in partial fulfillment of the requirements for a graduate degree from the University of North Dakota, I agree that the library of this University shall make it freely available for inspection. I further agree that permission for extensive copying for scholarly purposes may be granted by the professor who supervised my dissertation work or, in her absence, by the chairperson of the department or the dean of the Graduate School. It is understood that any copying or publication or other use of this dissertation or part thereof for financial gain shall not be allowed without my written permission. It is also understood that due recognition shall be given to me and to the University of North Dakota in any scholarly use which may be made of any material in my dissertation.

Signature 

Date April 24, 2007

TABLE OF CONTENTS

LIST OF TABLES.....	vi
ACKNOWLEDGMENTS	viii
ABSTRACT.....	ix
CHAPTER	
I. INTRODUCTION	1
II. METHODS AND PROCEDURES.....	35
III. STATUS OF SECURITY AWARENESS IN COLLEGES OF BUSINESS: AN ANALYSIS OF TRAINING, COURSEWORK, AND FACULTY PERCEPTIONS	45
IV. STATUS OF SECURITY AWARENESS IN ORGANIZATIONS: AN ANALYSIS OF TRAINING AND EDUCATION, POLICIES, AND SOCIAL ENGINEERING TESTING.....	66
V. CONCLUSIONS AND RECOMMENDATIONS	94
APPENDICES	104
Appendix A: Security Awareness in Colleges of Business Survey Instrument.....	105
Appendix B: Security Awareness in Organizations Survey Instrument.....	114
REFERENCES	126

LIST OF TABLES

Table	Page
1. Frequency and Percentages of Demographics in Colleges of Business	38
2. Frequency and Percentages of Demographics of Participants from Organizations	43
3. Frequency and Percentages for Security Awareness Training in Colleges of Business by Percent of Participants that Offer Training	54
4. Frequency and Percentages for Security Awareness Training Topics Covered in Colleges of Business by Percent of Participants that Offer Training	55
5. Frequency and Percentages for IT Security and Security Awareness Topics Integration by Departments in Business Core Courses.....	56
6. Rate of Coverage of Information Security and Awareness Topics in Colleges of Business Curricula.....	59
7. Frequency and Percentages for Security Awareness Training in Organizations by Percent of Total Participants	75
8. Frequency and Percentages for Tracking of Security Awareness Training by Percent of Organizations Offering Security Awareness Training	75
9. Frequency and Percentages for Reasons Security Awareness Training is not Offered in Organizations by Percent of Total Participants.....	76
10. Frequency and Percentages for Security Awareness Training Delivery Methods and Topics by Percent of Participants in Organizations Reporting Security Awareness Training Offered	77
11. Frequency and Percentages for Security Awareness Training by Percent of Participants in Organizations Reporting Security Awareness Training Offered.....	79

12.	Frequency and Percentages for Security Awareness Training by Percent of Participants in Organizations Reporting Security Awareness Training Offered	80
13.	Frequency and Percentages for Policies in Use by Percent of Participants in Organizations Completing Policy Section Questions	81
14.	Frequency and Percentages for Social Engineering Policies by Percent of Participants in Organizations Completing Policy Section Questions	82
15.	Mean Scores for Respondents' Level of Agreement with Statements on a Scale of 1 for Strongly Disagree to 5 for Strongly Agree	85

ACKNOWLEDGMENTS

My sincere appreciation and gratitude goes to my committee members: Dr. Richard Landry, my doctoral advisor, committee chair, and motivational statistics professor who taught me to like statistics, and patiently guided me through the dissertation process; Dr. Myrna Olson, whose enthusiasm for students and learning inspired me in the numerous teaching and learning courses; Dr. Sandy Braathen, who is a dear colleague and friend with a wonderful sense of humor who is always willing to answer a question when I need and a great source of support; and Dr. Jason Lane, who made History of Higher Education interesting and was always willing to answer my questions.

A special thank you goes to Justin Rotvold for his creative ideas and input into brainstorming this dissertation topic and his willingness to discuss the topic and answer questions from a practitioner point of view when I needed it. A thank you also goes to my mother, Margaret Stola, for her patience and encouragement during this educational journey.

Thank you also goes to the College of Business and colleagues from the ISBE department, who have provided continual encouragement and support during my PhD program and dissertation.

Finally, to Joel, my husband, my sincere appreciation for your patience and support during this process. Let's get out golfing, walking, or start planning a vacation.

ABSTRACT

The purpose of this study is twofold. The first purpose of this study is to investigate the status of security awareness training, IT-related policies, and the use of social engineering testing in business organizations. A second purpose of this study is to investigate the extent to which colleges and universities are offering security awareness topics as part of a student's coursework or daily activities, specifically in colleges of business, to help determine the level of students' security awareness exposure and preparedness for the work world.

The colleges of business study examined demographics, what topics were being covered, how often, to whom offered, and in what departmental areas the topics were being offered. Data was collected from 85 subjects across multiple departments from 35 states. The organizational study used partial matrix sampling to examine demographics, details and specific practices of security awareness training, policies, user compliance, auditing and testing, and user perceptions. Participants consisted of 144 professionals involved with management of information or records from all sizes and types of organizations. Descriptive statistics and MANOVAs were calculated on both data sets.

Results from the college of business study found that a substantial percentage of colleges of business may not offer security awareness training, but most faculty respondents recognized information security as an important concern and felt that students and faculty should receive more security awareness training. Although the study

found a significant percentage of participants that reported no integration of security awareness topics in the curriculum, almost one-third of total respondents would like to increase coverage of security awareness topics within their courses.

Results from the organizational study found that most organizations conduct security awareness training, but do not necessarily customize the format for different types of groups within the organization. Most respondents acknowledged information security as important, and felt motivated to follow security guidelines. The study revealed a need for increased use of social engineering policies, training, and testing along with a need to conduct periodic assessments of security awareness programs and components.

CHAPTER I

INTRODUCTION

Information security has become one of the most important and challenging issues facing today's organizations and consumers. Although many organizations are working hard to secure their information resources, numerous reports of information loss still occur every year. Keeping information secure is a complex and continuous task. The responsibility of keeping information secure, however, is not the responsibility of Information Technology (IT) security professionals alone; but rather, is the responsibility of all people within an organization. Therefore, all users not only should be aware of *what* their roles and responsibilities are in protecting information resources, but also should be aware of *how* they can protect information and respond to any potential security threat or issue. Security awareness programs address the need to educate all people in an organization so they can help to effectively protect the organization's information assets.

Several factors contribute to the challenge of keeping information secure. First, *pervasive use and dependence* on technology and the Internet may increase an organization's or a consumer's potential exposure to a variety of external security threats, because they involve communication outside of the physical boundaries and physical security of the organization. Statistics reveal that the number of Internet hosts is increasing at a steadily rapid pace. According to the January 2006 Internet Domain

Survey conducted by the Internet Systems Consortium, the Internet has increased from 72 million computers in January 2000 to 394 million in January 2006 (www.isc.org/ops/ds/reports/2006-01). The survey further indicates that the number of Internet hosts increased to 439 million hosts as of July 2006, a substantial increase of approximately 45 million hosts in just six months.

Second, increased *interconnectedness* to the world also has increased the exposure to potential external security threats (Thomson & von Solms, 1998). The computing environment has evolved from substantial use of dumb terminals in more restrictive mainframe environments to powerful workstations on the desktop in client/server environments. Increased remote access to corporate resources and increased access by suppliers in the supply chain has also changed the computing landscape. Consequently, information systems are no longer stand-alone systems that can be protected by simply locking doors and limiting access to information resources.

Third, the number and types of users has increased from a few data entry personnel to include almost all personnel at all levels of the organization including top management. Users now have a variety of computing skill levels, more computing power on their desktop, numerous software applications and development tools, mobile devices, and Internet access. Accessibility and availability of necessary information in real time is essential for decision making by management and for daily operations. Since users are becoming more sophisticated and need access to required information, physical and technical controls alone no longer are sufficient to maintain effective information security (Thomson et al., 1998). These characteristics of the computing environment have continued to intensify and will continue to accelerate well into the future. Therefore,

organizations, management, and users must employ additional methods to secure information and continually be on guard to help mitigate new types of risks to information compromise and loss. These additional methods may include practicing safe online behavior, knowing how to handle a potential security attack, following security policies, and following guidelines set out in security awareness training, just to name a few.

In higher education, increased use of electronic information, managing access to expanded sets of resources, and an increased threat matrix—including viruses, phishing, spyware, and theft of data--has added to the complexity of keeping its information assets secure (Dewey, DeBlois, & EDUCAUSE Current Issues Committee, 2006). Many of the same threats exist for education as they do for business organizations.

Need for the Study

Research has revealed that security awareness of end users is one of the most important links in any organization's security plan. "The security of any system is best seen as a chain of components, only as strong as the least secure one. Confidence, or assurance, is also a chain, as strong as the least trusted link. In each case the weakest component, be it computer or human, limits the effectiveness of all the others" (Cormack, 2001, p. 9). Since many breaches of security have been a result of people's actions within organizations, this study examines the status of information security awareness training and education, policies, user compliance, and social engineering testing in business organizations and colleges of business.

Various commercial entities have conducted periodic information security related surveys. A few well-known surveys include Ernst & Young Global Information Security

Survey, Computer Security Institute/Federal Bureau of Investigation (CSI/FBI) Computer Crime and Security Survey, and the Security Awareness Index survey conducted by PentaSafe Security Technologies. The latter reported the status of security awareness among organizations worldwide in 2002.

For almost a decade, the Ernst & Young survey has been distributed to executives, primarily Chief Security Officers (CSOs) and Chief Information Officers (CIOs), in global companies, government, and non-profit agencies. The Ernst & Young survey has examined key drivers for information security, trends, and also benchmarking information related to information security processes. Other well-known entities contract for a fee with organizations to provide data and benchmarking related to information security processes and practices.

In a 2004 survey by Ernst and Young, respondents named “lack of security awareness by users” as the top obstacle to effective information security and yet, only 28 percent listed security training or awareness as a top initiative in 2004. Since then much progress has been achieved. According to Ernst and Young’s 2006 survey, compliance is having an increasingly greater impact and is improving security; information security is more integrated into corporate cultures, increasingly proactive in meeting business objectives, and increasingly adopting standards (Ernst & Young, 2006).

Academic research in this area, however, is limited. Little or no research exists that examines the level of details and breadth of security awareness training, policies, compliance, testing, and perceptions covered by this study. Research needs to further examine security awareness and education of users to determine in greater detail what is being done, how it is being done, in addition to user perceptions and attitudes, and other

factors which are affecting information security so that further progress can be made toward improving the state of security awareness in all organizations. Statistical data obtained in this study may provide important details reflecting where organizations are in terms of maturity by various demographics. This information also could be applied to development, improvement, and implementation of various components in security awareness programs within various sizes and types of organizations. Also, the statistical data may help organizations to benchmark and compare how their security awareness programs match up with other peers or statistically similar organizations.

It is important to understand not only the status of security awareness, policies, and social engineering, but also the challenges and factors affecting achievement of an effective security awareness program within organizations and between demographically different types of organizations. This type of data could be useful to organizations to identify potential gaps in their security awareness programs, make improvements, or provide insight into components and characteristics of more formalized security awareness programs.

This study takes a more in-depth, comprehensive approach as compared to other studies by examining demographics, details and specific practices of security awareness training, policies, user compliance, auditing and testing (including social engineering testing), and user perceptions. Such a broad analysis contributes to the body of knowledge on the status of security awareness in organizations by also including a more detailed view of what organizations are doing, examining an extensive number of variables including social engineering, and providing additional information which can be used to improve current programs.

Another difference between this study and other studies is that the population for the organization survey is not comprised primarily of Chief Information Officers (CIOs) and Chief Security Officers (CSOs) as is the case in many other more commercial surveys. This study includes other individuals involved with management of information in various types of organizations. This perspective allows examination of security awareness from another angle and will help to determine if the same perception and knowledge of security awareness exists at other levels of the organization.

The combination of areas covered by this study also allows for additional statistical analyses of numerous and diverse variables. Statistical analysis also explores possible relationships between selected variables, and examines the maturity of security awareness programs in terms of implementation of best practices and successful security awareness program components. Examination of user opinions and beliefs also adds valuable insight as to the perception and importance of security awareness in organizations.

Security awareness training and education is not reserved for business organizations alone. Rather, information security awareness is necessary at all levels-- government, private, and general public (Hentea, 2005). Effective information security should be everyone's personal concern and priority. If security awareness is a top priority, it should permeate education as well as corporate and social culture. Little has been written about the status of security awareness training and education in our schools. Yet, education is one of the most effective methods to change behavior and prepare students for the real world.

Another unique aspect to this research is the inclusion of a second study that examines what departments in colleges of businesses are doing in terms of security awareness preparation and integration into the curriculum and activities for business students. With the importance of security awareness integration in organizations, it is important also to examine what is being taught to students to prepare them with these skills. Although some literature has discussed incorporation of information security curricula or degree programs aimed at Computer Science or IT-related majors, little or no literature exists regarding the status of security awareness inclusion and integration in the overall curricula of business students.

Some studies have examined motivational factors and attitudes affecting behavior and willingness to follow policies or other organizational guidelines. Stanton, Stam, Mastrangelo, and Jolton (2005) investigated end-user security behaviors and motivational antecedents and found relationships between key end user security behaviors and organization type, job role, organizational commitment, and job satisfaction. Lee (1995) examined factors that influence employees' willingness to comply with information security guidelines and procedures. Taneja (2006) studied behaviors and factors related to adverse usage of IS assets in which results supported the need for organizations to make major investments in education, training and awareness programs to improve security. Years of social psychology research has also provided considerable data regarding modification of behavior and motivation.

Other research has studied IT security in higher education by examining governance, strategy, and practices (Caruso, 2003) or current issues (Dewey et al., 2006), both giving an overall status as to IT security practices in colleges and universities.

Findings from a recent EDUCAUSE Center for Applied Research (ECAR) study in 2006, “Safeguarding the Tower: IT Security in Higher Education 2006” (Caruso, 2006), confirm that although much progress has been made to improve security programs within the last few years, less than 50 percent of the institutions surveyed regularly communicate security awareness issues to faculty, staff, and students and almost 95 percent still use weak username and password combinations.

From an instructional standpoint, a few studies also have examined undergraduates’ experience with IT and selected security behaviors. In the 2006 ECAR study of over 28,000 undergraduate students at 96 colleges and universities (most from four-year institutions), nearly 98 percent owned a PC, three-fourths of responding freshmen from four-year institutions owned laptops, almost one in five owned a personal digital assistant (PDA) or smart phone or both, more than one-third owned a wireless hub, and the average respondent reported spending 23 hours per week using various technologies, with business and engineering majors using IT more than others (Katz, 2006). With this level of technology use and connectedness to the Internet and online environment, there is a need for students to have a certain level of security awareness. The 2006 ECAR study (Katz, 2006) findings also suggest that even though younger students arrive with IT tools and self report a comfort level using IT for social and recreational purposes, they do not possess the same level of IT skills to support academic purposes.

Another study of 167 undergraduate students at two large public universities (Aytes & Connolly, 2004) revealed that although students considered themselves knowledgeable about safe computing behavior including protection from viruses,

computer crashes, and password violations, they continued to engage in unsafe computing or security behavior suggesting that awareness or knowledge does not guarantee safe computing behavior. Although students tended to recognize the potential negative consequences associated with risky computing behavior, they felt there was a low probability that these consequences would happen to them (Aytes et al., 2004). A contributing factor may be that in a university environment, upper management may not have the same level of control over technology users (students and faculty) as compared to a business organization; in academia, students experience little or no consequence for failure of technology security and faculty experience little or no punitive consequences for not complying with policies and no financial gain if they do comply (Perez, Berry, & Hollman, 2003).

A security awareness survey of 208 faculty, staff, and students (Perez et al., 2003) at a southern regional university found that there was some evidence that students were more familiar and comfortable practicing selected security measures than faculty in areas such as sharing files, setting file properties, smart cards, allowing other people to use one's computer, and installing a personal firewall. The survey (Perez et al., 2003) also showed that respondents were relatively familiar with basic security topics but were not very familiar with the more advanced topics such as firewalls, encryption, and smart cards.

With limited data available, it is unclear what departments in colleges of business specifically are doing to address the needs of students to develop security awareness skills and knowledge. Therefore, it is important to assess what higher education, especially colleges of business, are doing to educate their students and equip them with

the necessary skills to protect information resources. Higher education needs to adequately prepare its future graduates not only to know how to protect their own personal information but also the information of their future employers as well. Graduating students who are “security conscious” will benefit the organizations that hire them. According to Hentea (2005), if future graduates are to achieve information security awareness, it is necessary to offer one introductory course to teach basic security awareness methods to all university or college students. These future graduates will make up the work force that will be required to have information security skills (Hentea, 2005).

Another approach would be to integrate these topics across multiple disciplines. Faculty, however, would need to have adequate knowledge and skills to teach security-related topics. Assessment, therefore, is critical not only in understanding the current level of security awareness of students and faculty, but also critical in understanding the perceptions of faculty in colleges of business related to information security awareness and its inclusion in the curricula. Assessment also helps to provide a baseline from which to improve the status of security awareness in colleges of business.

Statement of Purpose

The overall purpose of this study is to examine the status of security awareness in organizations and departments within colleges of business. The status will reflect what both sides are doing in terms of training, delivery methods, and topics.

Additionally, the purpose of this study is twofold. The first purpose of this study is to investigate the extent to which colleges and universities are offering security awareness topics as part of a student’s coursework or daily activities, specifically in colleges of business, to help determine the level of students’ security awareness exposure

and preparedness for the work world. This part of the study also examines what topics are being covered, how often, to whom offered, and in what departmental areas the topics are being offered. A section of the survey also is devoted to current perceptions, behaviors, and level of importance given to security awareness within colleges of business.

The second purpose of this study is to investigate the status of security awareness training, IT-related policies, and the use of social engineering testing in business organizations. The investigation examines obstacles and factors in achieving effective information security to obtain a better understanding of the maturity of security awareness in organizations. The investigation also explores the differences and possible relationships between various demographic data and security awareness and user perception variables. A survey was administered to collect quantitative data to learn whether organizations are conducting security awareness training, what topics are being covered, and what types, if any, of social engineering tests are being conducted. The survey also addresses user perceptions, management support, and security-related user behavior.

Definition of Social Engineering

Social engineering attempts against unsuspecting individuals are a type of security threat which can result in significant data loss and which can be attributed to the actions and responses of people. For the purpose of this study, social engineering is defined as:

Successful or unsuccessful attempts to influence a person(s) into either revealing information or acting in a manner that would result in unauthorized access to, unauthorized use of, or unauthorized disclosure of

an information system, a network, or data. (Hansche, Beri, & Hare, 2004, p. 58).

Definition of Effective Information Security

A major goal of most or all organizations today is to achieve effective information security. Effective information security has been defined as “the result of a process of identifying an organization’s valued information assets, considering the range of potential risks to those assets, implementing effective policies addressing those specific conditions, and ensuring that those policies are developed, implemented, and communicated properly” (Hansche, Beri, Hare, 2004, p. 64). This definition of information security will be used for the purpose of this study.

Definition of Security Awareness

In relation to security, awareness has been defined as “being acquainted with, mindful of, conscious that and well informed of a specific subject, and thus implies knowing and understanding a subject and acting accordingly” (Wulgaert, 2005, p. 9). According to Wulgaert (2005), creating awareness involves more than pushing or communicating information to people, it “requires understanding, learning, acquiring skills and using the obtained knowledge,” (p. 9) of which the latter is critical to the success of the security awareness program. In other words, program success also depends on a change in peoples’ behavior. Training is the component that teaches the skills that organizations want users to learn and apply.

Definition of Security Chain

Security chain is a term occasionally mentioned in the literature, but seldom defined. An organization’s security is a line of security defenses or series of controls

collectively used to counteract security threats and keep information secure. According to the National Institute of Standards and Technology (<http://csrc.nist.gov/sec-cert/PPT/fisma.pdf>), links in the security chain can include a number of management, operational, and technical controls such as security policies and procedures, risk assessment, contingency planning, physical security, personnel security, security awareness and training, access control mechanism, identification and authentication mechanisms, encryption mechanisms, firewalls, intrusion detection systems, anti-viral software, audit mechanisms, and many others.

Definition of Security Culture

Ultimately, one of the goals of any security awareness program is to create a security culture. “Culture can be defined as a shared set of beliefs, values and behaviors among a community” (Cormack, 2001, p. 8). A strong security culture can strengthen the human link in the security chain.

Definition of Security Policies

In addition to technical security mechanisms, security also includes policies, procedures, and people. Security policies can be defined as “clear instructions that provide the guidelines for employee behavior for safeguarding information, and are a fundamental building block in developing effective controls to counter potential security threats” (Mitnick & Simon, 2002, p. 260).

Definition of Compliance

The term compliance can be used in two different contexts related to information security. In the first context, businesses and organizations may be required to adhere to legislative or regulatory mandates. This is referred to as regulatory compliance. Examples

of regulations that require compliance within the United States would include Sarbanes-Oxley, Health Insurance Portability and Accountability Act (HIPAA), Family Educational Rights and Privacy Act (FERPA), and the Gramm-Leach-Bliley Act. A second context would include user adherence to policies within an organization. This is referred to as user compliance. Although there may be a brief mention of regulatory compliance, the focus of this study will be on user compliance with security policies within an organization.

Overview of Information Security

As a first line of defense in implementing effective security programs, organizations have invested heavily in technologies such as firewalls, access control systems and authentication mechanisms, intrusion detection/prevention systems, anti-spyware and antivirus software, and encryption systems. Although these technological methods of protecting information may be effective in their respective ways, many losses are not caused by a *lack of* technology or *faulty* technology but rather are caused by *users* of technology and faulty *human* behavior (Mitnick & Simon, 2002; Orshesky, 2003; Im & Baskerville, 2005).

According to the 2006 Computer Security Institute/FBI (San Francisco Federal Bureau of Investigation) Computer Crime and Security survey (Gordon, Loeb, Lucyshyn, & Richardson, 2006), virus attacks continue to be the source of the greatest financial losses, followed by unauthorized access, losses related to laptops/ or mobile hardware, and theft of proprietary information collectively accounting for approximately 75% of the losses. All of these types of incidents have involved people using computers or accessing information. Although the survey (Gordon et al., 2006) indicated a dramatic decline in

total dollar losses per respondent, it also found that unauthorized access to information and theft of proprietary information showed significant increases in average dollar loss per respondent.

Since humans represent a vital component in organizational information systems, their role in any security plan should not be underestimated. It is sometimes forgotten that “computers and technology are merely tools, and that it is the human being that is using, configuring, installing, implementing, and abusing these tools” (Hansche et al., 2004, p. 57). Failure to comply with regulatory mandates, improper use of technology resources, failure to comply with organizational security policies, or exhibiting unsafe, risky security-related behaviors can result in regulatory penalties, loss of customer confidence/trust and business, loss of reputation, and loss of system integrity, availability, and confidentiality. The costs to an organization can be significant whether in dollars, trust, or perception.

Social Engineering

Users within an organization and their corresponding behavior are also primary targets for social engineering attacks. Social engineering attacks can be just as lethal for organizations as compared to other attacks, and therefore, deserve considerable attention and coverage in a security awareness program. Policies regarding social engineering are necessary. Policy takes judgment calls and decision-making regarding hacker requests out of the hands of the employee; if the request is prohibited by policy, the user must deny the request based on following policy (Thornburgh, 2004; Granger, 2002).

Social engineering derives much of its success to get the necessary information for an attack by preying on the helpful, trusting nature of most people or “individuals

who display signs of being susceptible to this psychological attack” (Hansche et al., 2004, p. 59). Examples of social engineering attempts can range from a person posing as a security officer or other authoritative figure to acting as a new hire who needs information or help from a person in a support position such as technical support or an administrative assistant.

Social engineers are very clever and deceptive. They can be quite skillful in applying a number of psychological principles that will lead an individual to give out information that he or she normally would not give out. Often, social engineers try to gain a person’s trust because people are more likely to give information to a person they trust. A wide variety of methods or combinations of methods can be used for a successful attack including active attacks that play on human emotion such as intimidation, impersonation, blackmail (including emotional blackmail), deception, flattery, befriending, authority, pressure, vanity, and sympathy (Peikari & Chuvakin, 2004) or passive attacks that do not interact with people but gather information through a variety of sources and provide a basis for future social engineering attacks.

A comprehensive approach to prevent social engineering attacks should include policies that utilize a classification system that specifies what information can be disclosed including to whom and by whom, in addition to procedures, awareness programs, training, and incident response plans (Thornburgh, 2004).

Users need to be aware of the forms that social engineering attacks can take, how they can occur, how they can prevent damage from occurring, and how to alert appropriate personnel of an attempted attack. By using a social *reengineering* approach, an approach also based on psychology, users can be taught the tricks played by criminals

and the behavioral risks to security not only making them aware of common social engineering practices and the psychology used but also making them alert to the risks of revealing critical information to hackers (Damle, 2002). An effective security awareness program should address these topics so that users are armed with the knowledge necessary to recognize a potential attack and how to prevent a breach from occurring. An effective program also needs to be ongoing so that users do not forget or let their guard down.

One study (Orgill, Romney, Bailey, & Orgill, 2004) found that during a social engineering test involving an auditor who presented a counterfeit questionnaire for users to answer, approximately 81% of those surveyed revealed their user name and 59% also revealed their password out of a total response rate of 92%. Alarmingly, only 12.5% asked for a piece of identification, and in addition, the auditor was also able to obtain all-hours keycard building access (Orgil et al., 2004). This study also showed that individuals who were alone were more easily manipulated, that those who trusted the auditor in part because of his/her name dropping of people in authority, were more likely to reveal information, and that training and education also helped prevent the social engineering attack.

Policies

Policies provide a critical framework and foundation to a security awareness program. They are clear instructions of behavior expected to help ensure security of information resources. They form the basis for security awareness training and the framework for compliance. Once written, policies must be communicated and then enforced in order to achieve effective information security. Employees must not only

know the security policies of the organization, but also must *understand* how vital the policies are in preventing damage from occurring (Mitnick et al., 2002).

Policies also need to be written at a level that all employees can understand. When communicating policies, it must be recognized that “Security is a portion of the entire business process and must use the words and objectives of the business units to be successful” (Peltier, 2005, p. 40). Policies need to articulate to employees why each policy is important. People not only need to know the importance but also the reasons why they should follow policies and how the policies will benefit them in their work. To help ensure compliance, employees need to know the damage that could occur as a result of noncompliance and the consequences for noncompliance (Mitnick et al., 2002). One method to help ensure user compliance is effective and continual monitoring of employees. However, employees should be informed of this monitoring process.

In addition to effectively communicating the consequences, procedures also need to be specified so that employees are aware of how to respond to an incident or threat to mitigate the risk or remove the threat. Employees should know how and to whom they should report a breach of security or attempted breach of security incident.

Once implemented, policies need to be regularly reviewed and updated to reflect changes in the organization’s needs and objectives, technological advances, and new security vulnerabilities and threats which arise (Mitnick et al., 2002). One of the most effective methods to communicate security policies and the security message is through an ongoing security awareness program.

Security Awareness Programs

The importance of an effective security awareness program cannot be overstated. Without the support of all people within the organization, any well designed security plan is significantly flawed. According to the Global Information Security Survey 2004 (Ernst & Young, 2004), respondents rated lack of users' security awareness as the greatest obstacle to effective information security.

While several organizations have implemented a security awareness program, there are still many organizations that have not. Other organizations may have implemented such a program but not to the degree that it has achieved its full potential. Although a number of factors may limit the implementation and growth of security awareness programs in organizations, lack of financial resources devoted to security awareness is one commonly cited reason.

Although there seems to be some consensus within organizations that security is important, that belief does not mean that adequate financial resources are allocated to fully support security awareness programs. The 2005 and 2006 CSI/FBI Computer Crime and Security Survey (Gordon et al., 2006) found that the majority of respondents agree that security awareness training is important, but on the average did not believe that their organization invests enough in security awareness (with the exception of high technology industries and government).

Higher education also seems to acknowledge that IT security is important but falls short in making security a priority or in developing and implementing formal security awareness programs. A 2003 ECAR survey of higher education institutions (Caruso, 2003) revealed that although 75% of respondents strongly agreed or agreed that

IT security ranked in the top three issues facing institutions, only 61% strongly agreed or agreed that IT security was a priority and only one-third had implemented a formal security awareness program for faculty, staff, and students. The survey findings (Caruso, 2003) also showed that the largest barrier to IT security was lack of resources as indicated by 71.7% of the respondents. In December, 2005, the seventh annual EDUCAUSE Current Issues Survey was conducted by the EDUCAUSE Current Issues Committee. For the first time, Security and Identity Management surpassed Funding IT as the top IT-related issue of strategic importance to institutions (Dewey et al., 2006).

Security curriculums in colleges and universities also have been very limited until recently thereby creating a challenge for businesses to find qualified security professionals. Historically, computer science programs offered very few, if any, security courses and most were more focused on encryption methodologies rather than dealing with the threats faced by corporations while the problem in business schools was that textbooks geared toward corporate security were not even available until late in 2002 (Panko, 2004). During the last two years, however, a number of universities have been implementing courses or degrees related to security.

Lack of financial resources is not the only factor influencing effective implementation of a strong security awareness program, however. Due to the complexity of keeping information assets secure, a comprehensive approach to effective information security is needed. In addition to performing a risk assessment and implementing technical and physical controls, administrative controls also must be implemented. Important administrative controls include: developing policies, communicating policies to users, user training, compliance, testing and auditing, and changing attitudes and

behavior--all of which are essential ingredients contributing to success of an effective information security program.

The importance of developing an effective security awareness program is not based solely for the purpose of communicating policies and procedures, however. Objectives of a security awareness program are also meant to help change user attitudes and behavior and therefore, should be structured to accomplish those goals and ensure user actions are security conscious (Thomson et al., 1998). As mentioned previously, not all security breaches have been the result of faulty technology or lack of technology. Many breaches have been the result of faulty *human* behavior, whether accidental or intentional. Unlike technology, a software patch cannot be created for human nature (Komiega, 2001). However, education and training can raise the awareness of users and build skills to strengthen the human link in the security chain. Education is one method of helping to change people's behavior. If security is to become part of everyone's job responsibilities, then it would seem reasonable to expect that users would be trained or educated as to what the risks are and how to mitigate those risks through safe security practices and behavior.

It is conceivable that a significant percentage of incidents could have been avoided if only people had been properly trained in what to watch for and how to respond.

Organizations also need to take a proactive role in educating users about the risks and proper ways to mitigate risks for new and emerging technologies before it becomes a serious problem. A recent security survey (Ernst & Young, 2005) found that approximately 50% of respondents recognize the information security concerns with

emerging *mobile* technologies but other emerging technologies such as voice-over IP telephony, open source, and server virtualization technologies receive only 21%, 10%, and 8% respectively even though those technologies also present serious threats. The survey (Ernst & Young, 2005) also found that although 42% of respondents report that new technologies will be a significant driver of information security within the next 12 months, over 25% of them have no plans to address the above-mentioned emerging technologies within the next 12 months. Yet, many of the risks associated with these technologies could be addressed through user awareness and training. Users at all levels need to be informed about the risks, impact of security issues, how to mitigate the risk, protect against loss, how to respond to an incident, and to whom to report a security breach.

Needs Assessment

Developing an IT Security Awareness and Training Program involves designing the program, developing the awareness and training material, and implementing the program (Wilson & Hash, 2003). It is well recognized that conducting a needs assessment, prior to designing any instructional course or training opportunity, is important to ensure that the course or training opportunity meets the needs of learners. In addition to helping determine users' awareness and training needs, the results of the needs assessment also can provide the necessary justification to convince top management to allocate sufficient resources to meet identified needs (Wilson et al., 2003). It is also important to recognize that implementation of any system or program must meet the mission and business goals of the organization. Key personnel

including top management, security personnel, IT support and system administration personnel, operational management, and system users need to be involved.

A comprehensive needs assessment can include examining available resource materials, analyses of any security breaches or events, changes to infrastructure, databases of users with access, findings from any oversight bodies, security plans, conversations with key personnel, and any special requirements such as technology or space requirements needed to conduct security awareness sessions and training (Wilson et al., 2003). Assessment is important at any phase of a security awareness program. Assessment can provide the information necessary to make decisions regarding initial design of a program or continual improvement of an existing program.

Awareness and Training Plan

Once a needs assessment has been completed, the information can be utilized to construct a plan for the development, implementation, and maintenance of a security awareness and training program. The National Institute of Standards and Technology (NIST) has outlined components that should be incorporated into a security awareness and training plan in their Special Publication 800-50 (Wilson et al., 2003). The components are summarized as follows:

1. Existing national and local policies that require awareness and training to be completed;
2. Scope of the program;
3. Roles and responsibilities of personnel involved with awareness and training material development, implementation, and maintenance, in addition to ensuring compliance of users to attend or read the material;

4. Identification of goals to be accomplished, target audiences, learning objectives, topics covered, deployment methods, documentation, feedback, evidence of learning, and evaluation and update of material for each aspect of the program;
5. Mandatory and/or optional courses or material for each target audience; and
6. Frequency of exposure to the material by each targeted audience.

Training

Training needs to be relevant, important, and tailored to each individual audience. “Attendees will pay attention and incorporate what they see or hear in a session if they feel that the material was developed specifically for them” (Wilson & Hash, n.d., Developing section ¶2). By focusing on how security can increase users’ productivity, make their jobs easier, solve their problems, or provide some other benefit, trainers make security personal, thereby increasing the effectiveness of the training and making it something users care about (Orchesky, 2003). Also, the message should be spoken in the audience’s language to ensure users understand the message (Desman, 2003).

Strategies for Successful Implementation and Maintenance

Although successful security awareness and training programs start with a well-defined plan, there are numerous other factors that significantly contribute to the success of the program. Critical success factors involved in achieving security awareness and developing a security culture include:

1. existence of a formal security awareness policy;
2. executive management support;
3. behavioral accountability;

4. formally assigned responsibility for security awareness activities;
5. involvement from multiple departments;
6. continuous security awareness activities;
7. clear objectives;
8. a formal security awareness program;
9. a security awareness message targeted to all people;
10. diversified delivery methods; and
11. a measurement of the effectiveness of the security awareness program.

(Wulgaert, 2005, p. 4)

Top management support is critical. Top management needs to be convinced of the value of security awareness programs in addition to the other security-related components such as risk analysis, policies, procedures, and business continuity planning (Peltier, 2005). Top management also needs to see the relationship between an effective security program and the information security triad of confidentiality, integrity, and availability which drives the security program (Peltier, 2005). Therefore, security professionals must sell their program and services by communicating how it supports the mission and business objectives of the organization and how it enables their audience—whether management, departments, or individuals—to do their job (Peltier, 2005).

When management is convinced of the program's value and become part of the process, they can and should be strong advocates and supporters of the program to convince the remainder of the employees in the organization to take it seriously. Employees will respond to authority figures, especially if those authority figures take an active role in support of the program. Lack of top management support, however, invites

weakness, causes policies to become unenforceable, and increases the probability that user behavior will not change (Ernst & Young, 2004).

Treating security and security awareness training as a continual process ensures that the information not only is current but also that the message is in constant focus, thereby increasing the effectiveness of the security awareness program. There are numerous strategies that can be used to assist in motivating users to keep attention and focus on security. One example is utilizing diversified delivery methods such as presentations, bulletin boards, email, cartoons, flyers, slogans, and newsletters among others to convey the message. Diversified delivery methods reach users in different ways and at different times on an ongoing basis.

Once user attention and focus are achieved, other factors also can contribute to an employee's willingness to follow security guidelines. Some of these factors include peer pressure (if other users are following policies), understanding the importance of compliance, use of small rewards for compliance, top management support, realistic goals and procedures, and application of social psychology methodology known to help change attitudes and behaviors. People may be more apt to follow guidelines of a program if they know it is well organized, well supported by all areas of the organization including top management, and if it is clear that the security awareness program will be around for a long time rather than just a fad that will go away in a few months. Understanding these factors and utilizing various motivators that capitalize on these factors to encourage compliance helps to yield positive results for the security awareness program.

Security awareness should involve all people in an organization. In addition, the security awareness message must be placed as a high priority and always be visible if a security culture is to be achieved. Security awareness training is not a one-time event. The security awareness process should begin with new employee orientation and continue until the employee leaves. At a minimum, all employees should be exposed to the security awareness message and material annually (Wilson et al., 2003).

Although it is important that users are aware of security issues including risks, threats, steps to mitigate risks, and procedures to report a security incident, “familiarity alone will not mitigate the risks associated with technology security issues” (Perez et al., 2003, p. 662). People must not only learn correct security procedures, but they must also practice them. Consequently, behavior also needs to be changed.

Organizations, therefore, need to incorporate methods and strategies that will help to change behavior and an employee’s willingness to follow security guidelines. Application of various social psychology techniques and principles can have a significant impact in making the program more effective and also in changing behavior (Thomson et al., 1998).

Security Culture

Whether in education or in business, to create *real* change means that “behavior has to be modified to such a degree that it becomes subconscious where people will carry out their daily activities in a security supporting manner,” (Thomson et al., 1998, p. 168) without having to think about what they are doing.

A strong security culture helps to promote acting in a security-conscious manner on a long-term basis because it becomes part of everyone’s shared beliefs and daily mode

of operation. Without a security culture “we cannot expect consistent behavior among those who operate and use our computers... Without a security culture to give confidence in the underlying systems, all these processes are being constructed on extremely fragile foundations” (Cormack, 2001, p. 10).

Compliance

Compliance involves adherence to policies. First and foremost, policies need to be accessible. Users cannot be held accountable for compliance with policies if they have not seen them, received or reviewed them, or agreed to comply with them through explicit or implicit agreements (Orchesky, 2003). Significant progress with policy development has been achieved in organizations that have implemented information security measures to comply with internal control regulations. According to Ernst and Young (2005), nearly 90% of these respondents focus on creating and updating policies and procedures, nearly 75% conduct training and awareness, and 81% view the information security function as important in supporting compliance with corporate policies and procedures.

Another strategy to help ensure compliance is to include information security into an employee’s job description. Making security awareness and compliance mandatory may reduce user apathy and encourage compliance because employees know that their behavior is being evaluated as part of periodic employee performance reviews and consequent salary increases (Schweitzer, 2005; Wulgaert, 2005). Monitoring tools can be employed to assist in the compliance process.

Other strategies to encourage compliance include the use of small rewards or trinkets, upper management support and commitment, and keeping the message in

constant focus. “There is no factor more influential than senior management setting the tone that information security is important and that individuals—including senior and middle management—will be held accountable for their actions” (Ernst & Young, 2004, p. 6); if senior management does not believe in it, the question of why users should follow it then arises. According to the 2004 Global Information Security (Ernst & Young, 2004), survey results indicated when senior management strongly valued information security, measures taken by the organization were more effective or confidence in them was high. Constant focus helps to ensure that users do not forget good security practices and helps to establish a security culture. It is important to create an environment that sends the message that practicing good security behavior not only will be an expectation but also a business necessity that will be around a long time.

Involving people from many departments may also help to solidify the foundation for implementation of a security awareness program. When users are involved in the process and contribute ideas they are likely to want to see the program succeed.

Monitoring, Auditing, and Testing

According to the 2006 CSI/FBI Computer Crime and Security Survey which surveyed 616 computer security practitioners in U.S. corporations, government agencies, medical institutions, universities and financial institutions (Gordon et al., 2006), 82% use security audits conducted by their internal staff as the most popular technique used to evaluate the effectiveness of information security. Over 50% also used penetration testing, automated tools, external security audits, email monitoring software, and web activity monitoring software.

Assessment

Once a security awareness program has been implemented, measuring and assessing the effectiveness of the organization's security awareness program is essential so that continual improvement and growth can occur. Improvement and growth, in turn, will allow for security awareness to be fully integrated in the organization, assisting in the overall maturation of the information security program.

Measurement helps to determine whether program and training objectives have been met as well as the amount of progress made in raising the security awareness of users. Measurement not only can find out whether the awareness program is effective, but also can help to identify any knowledge gaps and ensure the continuity and improvement of the overall security awareness program (Wulgaert, 2005).

Surveys, interviews, exams, and audits are a few of the more common assessment tools that can be used to measure progress. However, social engineering testing is another example of a successful method that can be used to measure effectiveness of the organization's security awareness program.

Feedback obtained from these assessments can then be used to provide direction in making modifications, improvements, or additions to the program. Assessment also needs to occur periodically so that the program can additionally accommodate the changes and new security issues that arise in such a dynamic environment.

Synthesis

Keeping information secure is a complex and continual process. Technologies change, security threats can increase or change, information access requirements by users may increase, access to selected information by business partners or members of the

supply chain may be required, and pervasive use of networks, software and development tools, and Internet access all add to the complexity of protecting information resources from numerous security threats. Not all threats are external, however. Many reports of security breaches or data loss have been due to the actions of insiders. Users have become an equally important link in the security chain as are various other physical, technical, and administrative controls. Therefore, a comprehensive approach is needed to ensure effective information security. An effective information security program needs to include development and implementation of policies, security awareness training, auditing and testing, compliance, and changing user behavior so that all users act in a security conscious manner.

Some research has been conducted on selected aspects of security. Limited research has been conducted on user behavior and attitudes in adhering to security procedures, or factors determining adverse usage of information systems assets. Years of research in social psychology has also focused on user behavior and attitudes which is useful when trying to positively change the security behavior of users. Commercial entities have conducted surveys in various areas of security ranging from drivers of security, current practices, number and types of security incidents to dollar losses caused by security incidents.

There has been limited academic research, however, regarding the status of security awareness programs, policies, and social engineering testing in organizations and its coverage in college curricula as a whole. Although information security textbooks are now being published and some colleges are implementing information assurance or security majors or degrees, little or no research addresses what colleges of business are

doing to prepare business students with security awareness knowledge and skills of business students in general. This two-phased study examines both of these areas in depth so that information obtained can be used improve the status of security awareness both in organizations and in colleges of business curricula.

Security Awareness in Organizations Research Questions

Questions addressed by this study include:

1. What is the status of security awareness training, IT-related policies, and the use of social engineering testing in business organizations?
2. What differences exist between selected demographic variables (type of organization, number of employees, United States geographic region, and department) and selected user perception and security awareness variables?
3. Is the perception of security among small organizations different than large organizations?

Colleges of Business Research Questions

1. What is the status of security awareness education in AACSB-accredited colleges of business?
2. What differences exist between selected demographic variables (department, number of enrolled students, United States geographic region, number of full-time faculty, level of technology support, and level of the college of business's use of technology) and selected security awareness education variables within AACSB colleges of business?
3. What relationships exist between selected security awareness and user perception variables?

Delimitations

This study contains the following delimitations:

1. This study focuses on security policies, procedures, education and testing and does not evaluate technical security tools and controls.
2. The population studied in education consists of department chairs in AACSB (Association to Advance Collegiate Schools of Business) accredited colleges of business and does not include students.
3. The populations studied in business organizations are business professionals that are members of ARMA International (Association of Records Managers and Administrators) within the United States. Members include but are not limited to records and information managers, MIS professionals, hospital administrators, imaging specialists, librarians, educators, and legal administrators.
4. Instruments used did not specifically test security awareness content knowledge.

Limitations

1. In the study involving department chairs from accredited colleges of business, since there was no way to control for multiple responses from the same institution, a small, but unlikely, possibility exists that a number of multiple responses came from the same institution.

Assumptions

In designing this study, the following assumptions were made:

1. The participants of AACSB-accredited colleges of business department chairs is representative of the entire group of department chairs from all United States AACSB-accredited colleges of business but not necessarily representative of all colleges of business in the United States regardless of accrediting body.
2. Participants understood the terminology used in the survey instrument.
3. Participants responded as accurately as possible to the survey instrument.

CHAPTER II

METHODS AND PROCEDURES

Because this dissertation is prepared in the two-article format, this chapter is divided into three parts. The first part describes procedures and methodology that were common to both studies. The second part describes procedures used for the colleges of business study, while the third part describes the procedures for the organizational study.

The procedures for this study were approved by the University of North Dakota Institutional Review Board (IRB) in July 2006. According to IRB procedures, subjects were free to choose whether or not to participate in the study. After performing a literature review and analyzing previous industry surveys, the researcher prepared two separate survey instruments—one for business organizations and one for colleges of business corresponding to the two different parts of the study. The estimated time needed to complete each survey was 20 minutes.

Both surveys were distributed in an online format through a web site with the site pages and data stored on a local college server. Secure Socket Layer (SSL) was used to establish a secure transmission. Each web site survey required participants to enter an email address solely for the purpose of identifying the record, thereby enabling responses to be saved after every screen and allowing participants the opportunity to return to the survey if they did not have all the information or time necessary to completely the survey on the first access. As soon as the data collection was complete, the email addresses were

deleted. Survey responses were stored in a secure, password-protected database on a local college server.

Accredited Colleges of Business Procedures and Methodology
Survey Instrument for Colleges of Business

The Security Awareness Survey for accredited colleges of business was constructed by the researcher to assess the status of security awareness in colleges of business through security awareness training and colleges of business academic course offerings. The survey instrument contained 38 questions, many of which contained multiple checkboxes to answer. The survey instrument contained questions related to demographics, course offerings, alternate security awareness education delivery formats, user perceptions, and attitudes/beliefs. The questions were organized into four sections: demographics, information security awareness training, security awareness education in coursework, security awareness training and education perceptions and beliefs (Appendix A).

The survey instrument was field tested with a small group of faculty from the local university. Appropriate modifications were made to the content based on the feedback received from this group. The instrument was also tested via the web to ensure that from an operational standpoint, electronic access to the instrument, delivery of individual questions to the respondent, acceptance of user responses utilizing various data validation controls, and transfer of responses to the database were all working properly. The web site was modified or edited and retested until operation of the site was successful. Data collection for this instrument occurred over a six week time period (mid December through the end of January).

The independent variables for the data set (AACSB colleges of business) consisted of numerous demographic variables that were self-reported and considered to be nominal variables. These variables included: number of students, state or United States geographic region, department, number of full-time faculty, level of technology support, and level of the college of business's use of technology. The dependent variables consisted of information security awareness training, security awareness education in coursework, security awareness training and education, and user perceptions and beliefs variables.

Sampling Procedures

An email was distributed to approximately 400 deans at Association to Advance Collegiate Schools of Business (AACSB) accredited colleges of business throughout the United States asking that they forward the request to participate in the Security Awareness survey to their department chairs or other appropriate department spokespersons. This procedure was used since there was no single e-mail distribution list or listserv for department chairs at AACSB-accredited colleges. A small number of email messages, less than 30, were returned for the following reasons: message was undeliverable, the person was no longer in that position or at that institution, the person was on leave, or the dean or appropriate spokesperson chose not to have their college participate.

The email described the study, its importance, and its purpose, in addition to containing a link to the online survey. A reminder email was sent approximately three to four weeks after the initial email. Since the original email was sent at a time when most colleges were getting close to final exam week followed by a significant holiday break,

the researcher felt it was appropriate to send a reminder once most colleges were back in session for the new calendar year. The potential number of participants was more difficult to quantify because there was not a fixed number of departments in every college of business, it was dependent on whether the dean would forward the message, and whether the dean chose only one spokesperson to reply.

Sample

In the final analysis, 85 subjects participated in the research survey. The percentage of participants from various departmental areas included accounting and finance (20.2%), information systems (29.8%), economics, management, and marketing (17.9%), and other which consisted of departments or combinations of departments not previously listed (32.1%). The enrollment of the colleges of business represented by the participants was to some extent, equally distributed across categories. A majority of the colleges represented in the survey reported less than 100 full-time college of business faculty (84.7%), fifteen or fewer faculty per department (74.1%), and greater than 70% tenure-track faculty members (79.5%) (Table 1).

Table 1. Frequency and Percentages of Demographics in Colleges of Business.

	N	%
Department		
Accounting and Finance	17	20.2
Information Systems	25	29.4
Economics, Management, and Marketing	15	17.9
Other	27	32.1

Table 1 (cont.)

	N	%
College of Business Enrollment		
Less than 1,000	13	15.3
1,001 to 1,500	20	23.5
1,501 to 2,000	16	18.8
2,001 to 3,000	15	17.6
Greater than 3,000	21	24.7
Region		
Mid-Continent East	18	21.2
Midwest	16	18.8
Northeast	14	16.5
Southern	20	23.5
West-Southwest	17	20.0
Full-time College of Business Faculty		
0 to 50	32	37.6
51 to 100	40	47.1
Greater than 100	13	15.3
Full-time Department Faculty		
0 to 5	14	16.5
6 to 10	23	27.1
11 to 15	26	30.6
16 to 25	13	15.3
Greater than 25	9	10.6
Percentage tenure-track full-time department faculty		
Less than 70	17	20.5
70 to 89	39	47.0
Equal to or greater than 90	27	32.5
College of business IT personnel and support services		
No	15	17.6
Yes	70	82.4
College of Business use of technology		
Average and Below Average	27	32.1
Above Average	39	46.4
High	18	21.4

Most survey participants reported that their college of business had its own Information Technology personnel and support services (82.4%). A majority of the participants also reported above average to high use of technology by their college of business (67.8%).

Summary

This part of the chapter presented the section areas covered in the Security Awareness survey instrument designed for colleges of business, along with the procedures used for distribution of the web-based survey. A detailed demographic analysis was also presented. The study included 85 faculty, department chairs, or deans across all department areas typically located in colleges of business. The next part of the chapter describes the methodology and procedures used in the organizational study.

Organizational Study Procedures and Methodology Survey Instrument for Business Organizations

The Security Awareness in Organizations survey instrument was constructed by the researcher to assess the demographics and status of security awareness in organizations. The survey instrument consisted of 69 questions organized into six sections including demographics, training, policies, compliance, auditing and testing, and user perceptions related to various aspects of information security awareness. The sections reflected key areas of security awareness programs, focused on what organizations are specifically doing, and included questions that probed attitudes and beliefs along with selected security-related behaviors of users involved with management of information.

The instrument was field tested with a small group of individuals to help ensure that questions were clear and concise. Appropriate modifications were made to questions

based on feedback received. The instrument was also tested via the web to ensure that from an operational standpoint electronic access to the instrument, delivery of individual questions to the participant, acceptance of user responses utilizing various data validation controls, and transfer of responses to the database were all working properly. Appropriate changes were made and the web-based survey was retested to ensure effective operation.

Since the survey instrument contained a large number of questions, many of which included multiple answers, the researcher decided to use a variation of matrix sampling, sometimes referred to as partial matrix sampling, so that the survey maintained a reasonable length for all participants to complete. All participants were required to complete the demographics, training, and auditing and testing sections. They were then randomly assigned either the policies and compliance sections or the user perceptions section (Appendix B). If, however, a participant responded with a 'no' to a question asking if training was conducted in his/her organization (which meant that the participant would skip fourteen additional questions on training), then he or she would receive all random sections. This procedure resulted in all participants completing an equivalent number of total questions and maintaining a reasonable time length for completion of the survey.

The independent variables for this data set from organizations consisted of numerous demographic variables that were self-reported and considered to be nominal variables. These variables include: type of organization, number of employees, state or United States geographic region, department and job responsibility. The dependent variables consisted of security awareness training, policies, compliance, auditing and testing, security awareness, and user perceptions variables. Some of the dependent

variables examined implementation, practices, methodology used in training, policies, compliance and auditing and testing. Other dependent variables examined user perceptions and behavior related to numerous areas of security awareness and information security.

Sampling Procedure

The researcher constructed an invitation to participate in the Security Awareness in Organizations survey which included the description, purpose and benefits. In mutual agreement between the researcher and professional organization, an email message inviting ARMA members to participate in the security awareness survey, along with a description of its purpose and a link to the survey was distributed by ARMA to its members so that only intended participants would respond. Two weeks after the initial email, a reminder email was sent. Data collection occurred over a one-month period beginning the last week of January, 2007 and ended March 1, 2007.

The sample population for this part of the study consisted of ARMA (Association of Records Managers and Administrators) International members primarily within the United States. The potential number of participants was approximately 9,000 people.

Sample

In the final analysis 144 subjects participated in the research survey. The percentage of participants came from a variety of organizational types including banking (4.2%), consulting (5.6%), education (9.2%), energy and utilities (13.4%), financial services (4.2%), government (22.2%), healthcare (4.2%), legal (7.7%), manufacturing (8.5%), and other (20.4%). Areas with two or less participants were added to the Other department category in addition to participants that did not fit into the above categories.

All sizes of organizations were represented, from less than 100 employees to greater than 50,000 employees, as well as all regions of the country (Table 2). A category named Other was used to group participants that did not specify a state, including those from Canada or other international sites. A majority of the respondents reported that their job duties or responsibilities involved working with Information Technology/Information Systems security, policies, or user training (82.6%). A majority of the respondents classified their job as a management position within the organization also (57.6%).

Table 2. Frequency and Percentages of Demographics of Participants from Organizations.

	N	%
Region		
Great Lakes	20	13.9
Great Northwest	8	5.6
Mid-Atlantic	13	9.0
Midwest/Rocky Mountain	21	14.6
Northeast	14	9.7
Pacific	19	13.2
Southeast	6	4.2
Southwest	19	13.2
Other	24	16.7
Type of Organization		
Banking	6	4.2
Consultant	8	5.6
Education	13	9.2
Energy and Utilities	19	13.4
Financial Services	6	4.2
Government	32	22.5
Healthcare	6	4.2
Legal	11	7.7
Manufacturing	12	8.5
Other	29	20.4

Table 2 (cont.)

	N	%
Number of Employees in Organization		
1 to 99	13	9.0
100 to 499	24	16.7
500 to 999	16	11.1
1,000 to 2,499	26	18.1
2,500 to 4,999	13	9
5,000 to 9,999	16	11.1
10,000 to 19,999	15	10.4
20,000 to 50,000	10	6.9
Greater than 50,000	11	7.6

Summary

This part of the chapter presented the section areas covered in the Security Awareness survey instrument designed for organizations, along with the procedures used for distribution of the web-based survey. A detailed demographic analysis also was presented. The study included 144 participants from all regions of the country, all sizes and types of organizations, many of whom were working with information technology/information systems security, policies, or user training. Over 50% of the participants' jobs were also classified as a management position.

CHAPTER III

STATUS OF SECURITY AWARENESS IN COLLEGES OF BUSINESS: AN ANALYSIS OF TRAINING, COURSEWORK, AND FACULTY PERCEPTIONS

Introduction

Keeping information secure in today's business world is a challenging and complex task. Business organizations are working hard to secure their information resources through numerous physical, technical, and administrative controls. Since many breaches of security have occurred as a result of people's actions, as opposed to the fault of technology, considerable attention has been focused recently on the security awareness of users at all levels of the organization. All users in the organization have the responsibility of keeping information secure. Security awareness programs address the need to educate all people in an organization so that they can effectively protect the organization's information assets.

A central mission for colleges of business is to prepare students with the knowledge and skills necessary for a variety of business careers. If information security is to be a part of everyone's job responsibility, it would be reasonable to expect that students would gain some of this background in their academic preparation.

Information security is not limited to business organizations. As a consumer, each student also should be concerned about protecting their information and taking appropriate security precautions with their own computing resources and information

assets when online. Information security awareness and skills, then, benefits students personally in addition to preparing them for a future career in business.

Although a number of post-secondary institutions have implemented information security or assurance degrees or programs over the past few years, it is unclear what is being done to integrate information security awareness into the curriculum or activities of *all* business students in colleges of business. This study arose in an effort to discover the status of security awareness integration by department into colleges of business and faculty perceptions regarding its incorporation.

Purpose

The purpose of this study was to investigate the extent to which colleges and universities are offering security awareness topics as part of a student's coursework or daily activities in colleges of business to help determine their level of security awareness exposure and preparedness for the work world. First, the study examined whether or not security awareness training was conducted for faculty and students and if it was conducted, what methods of delivery were being used. Second, the study examined coursework to learn what topics were being covered, how often, to whom offered, and in what departmental areas the topics were being offered. Finally, the study explored current faculty perceptions and the level of importance given to security awareness within colleges of business.

Review of Literature

Some studies have studied IT security in higher education from an organizational standpoint by examining governance, strategy, and practices (Caruso, 2003) or current issues (Dewey et al., 2006), yielding an overall status as to IT security practices in

colleges and universities as a whole. Findings from a recent EDUCAUSE Center for Applied Research (ECAR) 2006 study revealed that although much progress has been made to improve security programs within the last few years, less than 50 percent of the institutions surveyed regularly communicate security awareness issues to faculty, staff, and students.

A few studies also have examined undergraduates' experience with IT and selected security behaviors. In the 2006 ECAR study of over 28,000 undergraduate students at 96 colleges and universities (most from four-year institutions), nearly 98 percent own a PC, three-fourths of responding freshmen from four-year institutions own laptops, and the average respondent reports spending 23 hours per week using various technologies with business and engineering majors using IT more than others (Katz, 2006). Just as in business, with this level of technology use and connectedness to the Internet and online environment, there is a need for students to have a certain level of security awareness to protect their information resources.

A study of 167 undergraduate students at two large public universities (Aytes & Connolly, 2004) revealed that although students considered themselves knowledgeable about safe computing behavior, they continued to engage in unsafe computing or security behavior, which suggests that awareness or knowledge does not guarantee safe computing behavior. A contributing factor may be that in academia, students experience little or no consequence for failure of technology security, and faculty experiences little or no punitive consequences for not complying with policies and no financial gain if they do comply (Perez, Berry, & Hollman, 2003).

A security awareness survey of 208 faculty, staff, and students (Perez et al., 2003) at a southern regional university found some evidence that students were more familiar and comfortable practicing selected security measures than faculty.

With limited data available, it is important to assess what higher education, especially colleges of business, are doing to educate their students and equip them with the necessary skills to protect information resources. The purpose of assessment is to learn what is being done, evaluate to see if goals are being met or not, and determine if there are weak areas that need improvement. Feedback from an assessment will provide the needed information which then can be used to make modifications, or additions, that would strengthen and improve the security awareness program and security awareness in the curriculum so that it is effective in preparing students with information security awareness skills. Improving the security awareness program and education can help to create a security culture and ultimately help to change behavior so that students will act in a security conscious manner.

Higher education needs to adequately prepare its future graduates not only to know how to protect their own personal information but also the information of their future employers as well. Graduating students who are “security conscious” will benefit the organizations that hire them. These future graduates will make up the work force that will be required to have information security skills (Hentea, 2005). Examples include business graduates who may find themselves working for accounting firms who conduct audits of organizations’ security and controls, working in Information Systems departments or information security positions, or working as a manager who will need to be actively involved in supporting an organization’s security awareness program.

One approach to prepare students with security awareness knowledge is to teach an introductory security awareness course for all students. Another approach would be to integrate these topics across multiple disciplines. Faculty, however, then would need to have adequate knowledge and skills to teach security-related topics. Assessment, therefore, is critical not only in understanding the current level security awareness of students and faculty, but also critical in understanding the perceptions of faculty in colleges of business related to information security awareness and its inclusion in the curricula. Assessment could also help to provide a baseline from which to improve the status of security awareness in colleges of business.

Definition of Security Awareness

In relation to security, awareness has been defined as “being acquainted with, mindful of, conscious that and well informed of a specific subject, and thus implies knowing and understanding a subject and acting accordingly” (Wulgaert, 2005, p. 9). According to Wulgaert (2005), creating awareness involves more than pushing or communicating information to people, it “requires understanding, learning, acquiring skills and using the obtained knowledge,” (p. 9) of which the latter is critical to the success of the security awareness program. In other words, program success also depends on a change in peoples’ behavior. Training is the component that teaches the skills that organizations want users to learn and apply.

Definition of Security Culture

Ultimately, one of the goals of any security awareness program is to create a security culture. “Culture can be defined as a shared set of beliefs, values and behaviors among a community” (Cormack, 2001, p. 8).

Whether in education or in business, to create *real* change means that “Behavior has to be modified to such a degree that it becomes subconscious where people will carry out their daily activities in a security supporting manner,” (Thomson et al., 1998, p. 168) without having to think about what they are doing.

A strong security culture helps to promote acting in a security-conscious manner on a long-term basis because it becomes part of everyone’s shared beliefs and daily mode of operation. Without a security culture “we cannot expect consistent behavior among those who operate and use our computers... Without a security culture to give confidence in the underlying systems, all these processes are being constructed on extremely fragile foundations” (Cormack, 2001, p. 10).

Research Questions

1. What is the status of security awareness education by department in AACSB-accredited colleges of business?
2. What differences exist between selected demographic variables (number of enrolled students, United States geographic region, number of full-time faculty, level of technology support, and level of the college of business’s use of technology) and selected security awareness education variables within AACSB colleges of business?

Delimitations

1. The population studied in education consists of department chairs or appropriate spokespersons in AACSB (Association to Advance Collegiate Schools of Business) accredited colleges of business and does not include students.

2. Instruments used do not specifically test security awareness content knowledge.

Limitations

1. Since there was no way to control for multiple responses from the same institution, a small, but unlikely, possibility exists that a number of multiple responses came from the same institution.

Assumptions

In designing this study, the following assumptions were made:

1. The participants of AACSB-accredited colleges of business department chairs were representative of the entire group of department chairs from all United States AACSB-accredited colleges of business but not necessarily representative of all colleges of business in the United States regardless of accrediting body.
2. Participants understood the terminology used in the survey instrument.
3. Participants responded as accurately as possible to the survey instrument.

Procedures and Methods

The Security Awareness Survey for accredited colleges of business was constructed by the researcher to assess the status of security awareness by department in colleges of business through security awareness training and business course offerings. The survey instrument contained 38 questions, many of which contained multiple checkboxes to answer. The survey instrument contained questions related to demographics, course offerings, alternate security awareness education delivery formats, user perceptions, and attitudes or beliefs. The questions were organized into four

sections: demographics, information security awareness training, security awareness education in coursework, security awareness training and education perceptions and beliefs (Appendix A).

The independent variables for this data set consisted of numerous demographic variables which were self-reported and considered to be nominal variables. These variables included: number of students, state or United States geographic region, number of full-time faculty, level of technology support, and level of the college of business's use of technology. The dependent variables consisted of information security awareness training, security awareness education in coursework, security awareness training and education, and user perceptions and beliefs variables.

Sampling Procedures

An email was distributed to approximately 400 deans at AACSB-accredited colleges of business throughout the United States asking that they forward the request to participate in the Security Awareness Survey to their department chairs or other appropriate department spokespersons.

In the final analysis, 85 subjects from 35 states participated in the research survey. The percentage of participants from various departmental areas included accounting and finance (20.2%), information systems (29.8%), economics, management, and marketing (17.9%), and other which consisted of departments or combinations of departments not previously listed (32.1%). The enrollment of the colleges of business represented by the participants was to some extent, equally distributed across categories. A majority of the colleges represented in the survey reported less than 100 full-time college of business

faculty (84.7%), fifteen or fewer faculty per department (74.1%), and greater than 70% tenure-track faculty members (79.5%).

Most survey participants reported that their college of business had its own Information Technology personnel and support services (82.4%). A majority of the participants also reported above average to high use of technology by their college of business (67.8%).

Results

In an academic setting such as colleges of business, security awareness topics can either be addressed through training or coursework. For the purpose of this study, training is defined to include all non-credit coverage of security awareness topics varying widely in duration, content, and format. Security awareness education in coursework references courses offered by departments within colleges of business or by other departments outside the college of business.

Security Awareness Training

There was no significant difference by department on whether or not security awareness training was conducted. Therefore, the data was treated as a group, or combined.

The majority of survey participants reported that their colleges of business do not conduct security awareness training for faculty (60.0%) or students (62.4%). Also, there was no significant difference by any of the demographic variables on whether or not security awareness training was conducted.

When asked for reasons why security awareness training was not conducted, respondents did not overwhelmingly choose a particular reason. A breakdown of

responses by reasons and their respective percentages (of total participants) include: insufficient financial resources (21.2%), insufficient number of skilled staff (17.6%), lack of management commitment (17.6%), lack of management awareness (17.6%), and difficulty in determining the value of information security (9.4%). Approximately one-third, also, reported that security awareness training was not a high enough priority for resources (32.9%). A small number of individuals reported that training was conducted at the university level rather than a college of business level, and a small number of participants reported that they did not know why training was not conducted.

When security awareness training was conducted, respondents reported that IS staff is usually responsible for training (40.0%) as compared to management (12.7%), speakers (10.9%), and outsourcing (3.6%). Mandatory training for faculty, staff, and students was reported by 35.5% as well as tracking of attendance (35.5%). The most commonly used methods to deliver security awareness messages and training were email messages (43.1%), face-to-face training (39.2%), and newsletters (25.4%). (Table 3)

Table 3. Frequency and Percentages for Security Awareness Training in Colleges of Business by Percent of Participants that Offer Training.

	N	%
Mandatory Training		
Faculty and staff	11	35.5
Students	11	35.5
Attendance		
All personnel	14	28.0
Faculty	10	20.0
Students	8	16.0
Administration	8	16.0

Table 3 (cont.)

	N	%
Attendance (cont.)		
IS Staff	8	16.0
Administrative support	7	14.0
Tracking of Attendance		
Yes	11	35.5
Security Awareness Training Delivery Methods		
Email messages	22	43.1
Face to face	20	39.2
Newsletters	13	25.4
Online training	7	13.7
Posters, flyers	4	7.8
Presentations, speakers	3	5.9
Mail stuffers	3	5.9
CD-ROM/DVD	2	3.9
Videos	1	1.9

Security awareness topics covered in training most frequently included viruses (50.9%), password protection (50.9%), email security (49.0%), internet security (47.1%), confidentiality (41.2%), and acceptable use (35.2%) (Table 4).

Table 4. Frequency and Percentages for Security Awareness Training Topics Covered in Colleges of Business by Percent of Participants that Offer Training.

	N	%
IT Security Awareness Training Topics Covered		
Viruses	26	50.9
Password protection	26	50.9
Email security	25	49.0
Internet security	24	47.1
Confidentiality	21	41.2

Table 4 (cont.)

	N	%
IT Security Awareness Training Topics Covered (cont.)		
Acceptable use	18	35.2
Workstation security	15	29.4
Spyware	13	25.5
Downloading shareware software	13	25.5
Remote access	12	23.5
Service pack or OS updates	10	19.6
Information sensitivity and classification	9	17.6
Bringing in home software	8	15.7
Incident reporting	7	13.7
Specialized security (ex: HIPAA, FERPA)	7	13.7
Identity theft	6	11.8
Social engineering	5	9.8
Risk assessment	5	9.8

Security Awareness in Coursework

Coverage of security awareness topics offered in business curricula courses was examined. The top five IT security and security awareness topics integrated into business core courses included viruses (50.6%), password protection (46.9%), email security (46.9%), confidentiality (42.0%), and acceptable use (37.0%) (Table 5).

Table 5. Frequency and Percentages for IT Security and Security Awareness Topics Integration by Departments in Business Core Courses.

	N	%
Topics integrated into business core courses		
Viruses	41	50.6
Password protection	38	46.9
Email security	38	46.9
Confidentiality	34	42.0
Acceptable use	30	37.0

Table 5 (cont.)

	N	%
Identity theft	28	34.6
Internet security	26	32.1
Spyware	26	32.1
Downloading shareware software	23	28.4
Security threats	23	28.4
Information sensitivity and classification	22	27.2
Internal controls—process controls	22	27.2
Workstation security	22	27.2
Bringing in home software	21	25.9
Remote access	21	25.9
IT Security controls—technical	21	25.9
IT governance	19	23.5
IT/Security policy development	18	22.2
Social engineering	17	21.0
Risk assessment	16	19.8
Top management role in security program	16	19.8
IT Security controls—human safeguards	16	19.8
No security awareness topics integrated	16	19.8
Service pack or OS updates	15	18.5
IT security controls—administrative/data	14	17.3
Specialized security (ex: HIPAA, FERPA)	9	11.1
Incident reporting	8	9.9

Integration of IT security and security awareness topics within each department's courses, however, was relatively low. The majority (68.2%) of respondents reported less than 25% integration (48.2%) or no integration (20.0%). Only one percent reported 75% or greater integration, while 10.6% reported 25-49% integration and the same percentage for 50 to 74% integration. A one-way MANOVA was calculated that examined the differences by department on percentage of integration within department courses and level of department graduates' preparedness on security awareness topics. A significant effect was found ($\Lambda(6,136) = 2.27, p < .05$). Follow-up univariate ANOVAs

indicated that preparedness of graduates was not affected by department ($F(3,69) = 1.02$, $p > .05$). As might be expected, level of security awareness integration within courses was affected by department ($F(3, 69) = 4.11$, $p = .01$). A Bonferroni post hoc analysis revealed that the percentage of integration was significantly higher for Information Systems ($M = 1.71$, $sd = .19$) than Economics, Management and Marketing ($M = .75$, $sd = .25$). Other than the one significant difference showing Information Systems had more integration than Economics, Management, and Marketing (combined), there was no significant difference by department in preparedness of graduates or level of integration with or between other departments.

Within departments' major courses, the rate of moderate coverage was 30.0% while significant to extensive coverage was 13.8%. Rate of coverage in elective courses was slightly less with 27.5% reporting moderate coverage, and 11.3% significant to extensive coverage. In other college of business courses, respondents reported 37.5% moderate coverage and 6.3% significant to extensive coverage. Courses outside the college of business reported less coverage with 31.3% reporting moderate coverage, and 1.3% significant coverage. The majority of departments' electives reported no coverage (51.3%) and courses outside the college of business were reported to have 53.8% with no coverage.

Table 6. Rate of Coverage of Information Security and Awareness Topics in Colleges of Business Curricula.

	N	%
Department elective courses		
Significant to Extensive	9	11.3
Moderate	22	27.5
Special Unit	8	10.0
Not Covered	41	51.3
Department major courses		
Significant to Extensive	11	13.8
Moderate	24	30.0
Special Unit	11	13.8
Not Covered	34	42.5
Other college of business courses		
Significant to Extensive	5	6.3
Moderate	30	37.5
Special Unit	9	11.3
Not Covered	36	45.0
Outside college of business courses		
Significant to Extensive	1	1.3
Moderate	25	31.3
Special Unit	11	13.8
Not Covered	43	53.8

Perceptions and Beliefs

Faculty perceptions and beliefs regarding security awareness training and education were also surveyed. Results revealed that a majority of business faculty disagreed or strongly disagreed that information security and awareness topics should be taught only by the Information Systems department faculty (55.8%), and also disagreed that it should be taught only in Information Systems courses (64.9%). However, faculty

did agree or strongly agree that information security and awareness should be taught *primarily* in IS courses (61.0%).

A greater percentage of faculty members believed that there was not a security culture within their college (49.4%) as compared to 23.4% who felt there was a security culture. Computer and information security, however, was an important concern to faculty (56.8%). Faculty felt that they should receive more information security and awareness training (71.1%) and that students should receive more information security and awareness education (71.1%).

Faculty had mixed feelings regarding whether or not graduating students were prepared to meet the security challenges in today's work world. Only 19.7% of faculty agreed that students were prepared as compared to 35.5% who disagreed or strongly disagreed that students were prepared to meet the security challenges. The remaining percentage (44.7%) had no opinion or felt it was not applicable.

Results also showed that faculty believed security is not primarily a technical issue (63.5%). They also believed that people are equally as important to security as technology (91.7%). Both of these statistics represent positive findings.

Pearson correlation calculations examined selected variables including security awareness training for students, perception of how well prepared graduating students are in security awareness topics, importance of information security and awareness knowledge in the business student's curriculum, security culture, integration of information security into business courses, whether information security was an important concern for faculty, and whether students should receive more information security and awareness education for possible relationships.

The Pearson correlation coefficient calculation revealed a moderate, positive correlation between security awareness preparedness of graduating students and perceived existence of security culture within their college ($r(70) = .36, p < .01$), whether security awareness training was conducted for students ($r(73) = .35, p < .01$), and the importance of security awareness knowledge in the business students' curriculum ($r(72) = .33, p < .01$). The significant relationship between these variables indicated that faculty who rated graduating students' level of preparedness in security awareness knowledge higher tended to be from a college of business that conducts security awareness training for students, believed a security culture existed in their college, and considered information security awareness and knowledge important in the business curriculum.

The need for greater security awareness education was moderately, negatively correlated with security culture ($r(74) = -.30, p < .01$), indicating that if faculty perceived a security culture existed within their college, they tended to feel less of a need for a greater amount of security awareness education. A moderate, positive correlation was found between the need for greater security awareness education and the belief of whether security awareness topics should be integrated into the business students' curriculum ($r(74) = .38, p < .01$). Faculty who felt there was a need for greater security awareness education tended to believe security awareness should be integrated into the business students' curriculum.

Other slight, positive correlations with a significant relationship were also found. Faculty that perceived a security culture existed within their college tended to be from a college where security awareness training was conducted ($r(75) = .25, p < .05$) and where security awareness was an important concern for faculty ($r(74) = .29, p < .05$).

Importance of information security and awareness knowledge in the curriculum had a slight, positive correlation with four variables: colleges that conduct security awareness training for students ($r(84) = .29, p < .05$), a belief that students should receive more security awareness education ($r(70) = .24, p < .05$), security awareness is an important concern for faculty ($r(68) = .29, p < .05$).

A slight, positive correlation also was found between whether information security was an important concern for faculty and how well students were prepared in security awareness topics ($r(67) = .25, p < .05$) indicating that faculty who believed security awareness was important tended to rate students' level of security awareness preparedness higher.

Discussion

The majority of participants in this study agreed that computer and information security was an important concern. Furthermore, they also believed that faculty and students should receive more information security and awareness training. Although participants believed security awareness was important, the majority reported that their college did not offer training for faculty (60.0%) or students (62.4%). These numbers seem to support findings from other research studies; however, the numbers do not reflect whether any awareness training is conducted elsewhere in the university or four-year institution. Recent findings from a 2006 ECAR study confirms that although much progress has been achieved, less than 50 percent of institutions surveyed regularly communicate security awareness issues to faculty, staff, and students.

Two of the reasons receiving the highest percentage of response for training not being conducted were lack of financial resources (21.2%) and security awareness training

not being a high enough priority for resources (32.9%). These findings are similar to a 2003 ECAR survey of higher education institutions that revealed that although 75% of respondents strongly agreed or agreed that IT security ranked in the top three issues, only 61 percent strongly agreed or agreed that IT security was a priority and only one-third had implemented a formal security awareness program for faculty, staff and students (Caruso, 2003). The ECAR study also found the largest barrier to IT security was lack of resources as indicated by 71.7% of the respondents.

A significant percentage of participants still report no integration of information security and awareness topics in department major courses (42.5%), elective courses (51.3%), other business courses (45.0%), and courses outside the college of business (53.8%). These numbers would suggest there is ample opportunity to improve the status of security awareness coverage in the business curricula. The percentage of faculty that views security awareness knowledge as important in the business curricula also could be increased. Although a majority viewed these topics as important, a substantial 36.8% did not view them as important. Increasing the amount of training and education for faculty may help to increase the numbers of faculty that view security awareness as important.

A very positive finding was that faculty participants overwhelmingly consider people equally important to security as technology. They also believe that both they and students should receive more education and training, and tend to believe that students are not as prepared as they could be. These attitudes should help provide positive momentum to continue to raise the status of security awareness in colleges of business. Although the Information Systems department is viewed as the primary source of these offerings, it is not believed to be the only department that should offer coverage. Approximately 30%

would like to increase coverage of information security and awareness topics within their courses which should help to increase the percentage of integration in the business curricula.

Implications

Although security awareness progress seems to have been achieved, findings from this study indicate that 60% of colleges of business still do not conduct security awareness training for faculty or students, suggesting that a need still exists to integrate more security awareness training into colleges of business. Training also helps to change attitudes and behavior. Also, only 20% of faculty believed that students were prepared to meet the security challenges of today's business world, suggesting that additional training and education might be needed to better prepare students.

Faculty are required to protect a variety of information resources; yet, topics such as incident reporting, specialized security including FERPA, and risks assessments received very limited coverage (less than 10%) in security awareness training, if training was offered at all. This represents an area of concern that should be examined to improve the status of security awareness. The limited coverage or integration within coursework of these same topics plus top management's role in a security program also would suggest that these areas should be examined for possible inclusion in the curriculum. In addition, a detailed assessment could be conducted within each college which would help to establish a baseline and map of current topics and offerings from which progress then could be made.

The statistical data supports the notion that security awareness training and education tend to contribute to people's positive perception of security preparedness

within the organization. Participants that believe there is a security culture within their college of business also tend to believe that students' level of security preparedness is higher, their college conducts security awareness, and their rating of security coverage and importance in the business curriculum is higher.

CHAPTER IV

STATUS OF SECURITY AWARENESS IN ORGANIZATIONS: AN ANALYSIS OF TRAINING AND EDUCATION, POLICIES, AND SOCIAL ENGINEERING TESTING

Introduction

Information security has become one of the most important and challenging issues facing today's organizations. With pervasive use of technology and widespread connectedness to the global environment, organizations have increasingly become exposed to numerous and varied threats. Technical controls can provide substantial protection against many of these threats, but they alone do not provide a comprehensive solution. Although these technological methods of protecting information may be effective in their respective ways, many losses are not caused by a *lack of* technology or *faulty* technology but rather are caused by *users* of technology and *faulty human* behavior (Mitnick & Simon, 2002; Orshesky, 2003; Im & Baskerville, 2005). People, then, not only can be part of the problem, but also they can and *should be* part of the solution. People need to be an integral part of any organization's information security defense system.

Keeping information secure is not only the responsibility of Information Technology security professionals, but also the responsibility of *all* people within the organization. Therefore, all users should be aware not only of *what* their roles and responsibilities are in protecting information resources, but also should be aware of *how*

they can protect information and respond to any potential security threat or issue.

Security awareness programs address the need to educate all people in an organization so they can help to effectively protect the organization's information assets.

Although many organizations have implemented security awareness programs and have achieved progress in improving the security awareness of all the employees, others may not have developed a formal security awareness program yet. Sometimes it is difficult to know exactly how much progress has been realized across all types and sizes of organizations, and how well the information security goals and message have been communicated across all levels of the organization. This study arose in an effort to discover the status of security awareness programs in addition to methods and best practices used, testing, and user perceptions.

Purpose

The purpose of this study was to investigate the status of security awareness training, IT-related policies, and the use of social engineering testing in business organizations. The organizational investigation also examined obstacles and factors in achieving effective information security to obtain a better understanding of the real status of security awareness in organizations. The organizational investigation also explored the differences and possible relationships between various demographic data and security awareness and user perception variables.

Review of Literature

Research in the area of information security has taken numerous and varied approaches. Some research has looked at the technical aspect, others at the behavioral side, in terms of changing people's behavior or motivation to follow security guidelines.

Various commercial entities also have surveyed their clients or other organizations on various aspects of information security. Many of these studies have targeted chief information officers, chief security officers, and other top level security professionals and executives in organizations both in the United States and across the globe. Two well known information security surveys conducted on a regular basis include the CSI/FBI Computer Crime and Security Survey and Ernst & Young's Global Information Security Survey. Since information security is part of a very dynamic and changing environment, results can change on a yearly basis based on changes in the business environment, regulations and compliance, new technologies, and new issues or threats that arise.

In a 2004 survey by Ernst and Young, respondents named "lack of security awareness by users" as the top obstacle to effective information security and yet, only 28 percent listed security training or awareness as a top initiative in 2004. Since then much progress has been achieved. According to Ernst and Young's 2006 Global Information Security Survey, information security is being strengthened within organizations and maturing, compliance is having an increasingly greater impact and is improving security; information security is more integrated into corporate cultures, increasingly proactive in meeting business objectives, and increasingly adopting standards (Ernst & Young, 2006).

The 2006 CSI/FBI Computer Crime and Security Survey found that most organizations view security awareness as important, and there have been substantial increases in perception of its importance (Gordon, Loeb, Lucyshyn, & Richardson, 2006). The survey also found that virus attacks continue to be the source of the greatest financial losses, followed by unauthorized access, losses related to laptops/ or mobile hardware, and theft of proprietary information, collectively accounting for approximately 75% of

the losses. All of these types of incidents have involved people using computers or accessing information. Although the survey (Gordon et al., 2006) indicated a dramatic decline in total dollar losses per respondent, it also found that unauthorized access to information and theft of proprietary information showed significant increases in average dollar loss per respondent.

Significant progress with policy development has been accomplished in organizations that have implemented information security measures to comply with internal control regulations. According to Ernst and Young (2005), nearly 90% of these respondents focused on creating and updating policies and procedures, nearly 75% conducted training and awareness, and 81% viewed the information security function as important in supporting compliance with corporate policies and procedures.

According to the 2006 CSI/FBI Computer Crime and Security Survey which surveyed 616 computer security practitioners in U.S. corporations, government agencies, medical institutions, universities and financial institutions (Gordon et al., 2006), 82% used security audits conducted by their internal staff as the most popular technique used to evaluate the effectiveness of information security. Over 50% also used penetration testing, automated tools, external security audits, email monitoring software, and web activity monitoring software.

With limited academic research in this area, it was important to assess in greater detail what was being done, how it was being done, along with user perceptions and attitudes so that further progress can be achieved toward improving the state of security awareness in all organizations. A key difference between this study and other studies is that this study did not target the CIOs and CSOs, but rather other individuals involved

with management of information in various types of organizations, thereby examining security awareness from a different perspective and angle.

The statistical analysis can be useful to organizations to identify potential gaps in their security awareness programs, make improvements, or provide insight into components and characteristics of more formalized security awareness programs.

This study takes an in-depth, comprehensive approach by examining demographics, details and specific practices of security awareness training, policies, user compliance, auditing and testing (including social engineering testing), and user perceptions. This broad analysis adds to the body of knowledge regarding the status of security awareness within organizations and provides an analysis of how other levels and types of users perceive security awareness within organizations. This information then can be used to improve organizations' security awareness programs, benchmark progress against other organizations, and provide insight into the maturity of organizations' security awareness programs.

Definition of Security Awareness

In relation to security, awareness has been defined as “being acquainted with, mindful of, conscious that and well informed of a specific subject, and thus implies knowing and understanding a subject and acting accordingly” (Wulgaert, 2005, p. 9). According to Wulgaert (2005), creating awareness involves more than pushing or communication information to people, it “requires understanding, learning acquiring skills and using the obtained knowledge,” (p. 9) of which the latter is critical to the success of the security awareness program. In other words, program success also depends on a change in peoples' behavior.

Definition of Security Culture

Ultimately, one of the goals of any security awareness program is to create a security culture. “Culture can be defined as a shared set of beliefs, values and behaviors among a community” (Cormack, 2001, p. 8).

Real change means that “Behavior has to be modified to such a degree that it becomes subconscious where people will carry out their daily activities in a security supporting manner,” (Thomson et al., 1998, p. 168) without having to think about what they are doing.

Definition of Social Engineering

Social engineering attempts against unsuspecting individuals are a type of security threat which can result in significant data loss and which can be attributed to the actions and responses of people. For the purpose of this study, social engineering is defined as:

Successful or unsuccessful attempts to influence a person(s) into either revealing information or acting in a manner that would result in unauthorized access to, unauthorized use of, or unauthorized disclosure of an information system, a network, or data. (Hansche, Beri, & Hare, 2004, p. 58)

Research Questions

1. What was the status of security awareness training, IT-related policies, and the use of social engineering testing in business organizations?
2. What differences existed between selected demographic variables (type of organization, number of employees, and United States geographic region) on selected user perception and security awareness variables?

3. Was the perception of security among small organizations different than large organizations?

Delimitations

1. This study focused on security awareness training, policies, procedures, and testing and did not evaluate technical security tools and controls.
2. The population studied in organizations consisted of business professionals that are members of ARMA International (Association of Records Managers and Administrators) primarily within the United States. Members included but were not limited to records, document, and information managers, MIS professionals, legal administrators, archives, administrators, and educators.
3. Instruments used did not specifically test security awareness content knowledge.

Assumptions

In designing this study, the following assumptions were made.

1. Participants understood the terminology used in the survey instrument.
2. Participants responded as accurately as possible to the survey instrument.

Procedures and Methods

The Security Awareness in Organizations survey instrument was constructed by the researcher to assess the demographics and status of security awareness in organizations. The survey instrument consisted of 69 questions organized into six sections including demographics, training, policies, compliance, auditing and testing, and user perceptions related to various aspects of information security awareness. The sections reflected key areas of security awareness programs, focused on what

organizations are specifically doing, and included questions that probed attitudes and beliefs along with selected security-related behaviors of users involved with management of information.

Since the survey instrument contained a large number of questions, many of which included multiple answers, the researcher decided to use a variation of matrix sampling, sometimes referred to as partial matrix sampling, so that the survey maintained a reasonable length for all participants to complete. All participants were required to complete the demographics, training, and auditing and testing sections. They were then randomly assigned one or more sections from the policies, compliance and user perceptions sections (Appendix B).

The independent variables for this data set from organizations consisted of numerous demographic variables which were self-reported and considered to be nominal variables. These variables included: type of organization, number of employees, state or United States geographic region, department and job responsibility. The dependent variables consisted of security awareness training, policies, compliance, auditing and testing, security awareness, and user perceptions variables. Some of the dependent variables examined implementation, practices, methodology used in training, policies, compliance and auditing and testing. Other dependent variables examined user perceptions and behavior related to numerous areas of security awareness and information security.

Sampling Procedures

In mutual agreement between the researcher and professional organization, an email message inviting ARMA members to participate in the security awareness survey,

along with a description of its purpose and a link to the survey was distributed by ARMA to its members so that only intended participants would respond. The sample population for this part of the study consisted of ARMA (Association of Records Managers and Administrators) International members primarily within the United States. The potential number of participants was approximately 9,000 people.

In the final analysis 144 subjects participated in the research survey. The percentage of participants came from a variety of organizational types including banking (4.2%), consulting (5.6%), education (9.2%), energy and utilities (13.4%), financial services (4.2%), government (22.2%), healthcare (4.2%), legal (7.7%), manufacturing (8.5%), and other (20.4%). A category named Other was used to group participants that did not specify a state, including those from Canada or other international sites.

A majority of the respondents reported that their job duties or responsibilities involved working with Information Technology/Information Systems security, policies, or user training (82.6%). A majority of the respondents classified their job as a management position within the organization also (57.6%).

Results

Result categories mirror the sections covered by the survey instrument: security awareness training, policies, auditing and testing, and security awareness and user perceptions.

Security Awareness Training

The majority of survey participants reported that their organizations do conduct security awareness training (59.9%), which leaves 40% of organizations responding that they do not offer or do not know if security awareness training is offered. The percentage

of organizations that mandated security awareness training, however, was more evenly split. Mandatory training was reported by 44.7%, while the same percentage (44.7%) did not mandate training and 10.7% did not know (Table 7).

Table 7. Frequency and Percentages for Security Awareness Training in Organizations by Percent of Total Participants.

	N	%
Is security awareness training offered		
Yes	85	59.9
No	46	32.4
Do not know	11	7.7
Is security awareness training mandatory		
Yes	63	44.7
No	63	44.7
Do not know	11	7.7

When asked if security awareness training was tracked, 72.8% of the participants from organizations where security awareness training is offered reported yes, 11.1% reported no, 16.0% did not know (Table 8).

Table 8. Frequency and Percentages for Tracking of Security Awareness Training by Percent of Organizations Offering Security Awareness Training.

	N	%
Is attendance at security awareness training tracked		
Yes	59	72.8
No	9	11.1
Do not know	13	16.0

Calculations from three one-way MANOVAs found no significant difference by type of organization, number of employees, or region on three dependent variables: whether security awareness training was offered, if the training was mandated, and if attendance at security awareness was tracked.

The most commonly reported reasons for security awareness training not being conducted were: lack of awareness by management (13.9%), lack of management support or commitment (11.8%), belief that end users are skilled, know how to use a computer, or know better (11.8%), and security awareness training not a high enough priority for resources (11.1%).

Table 9. Frequency and Percentages for Reasons Security Awareness Training is not Offered in Organizations by Percent of Total Participants.

	N	%
Lack of management awareness	20	13.9
Lack of management support/commitment	17	11.8
End users are skilled or know better	17	11.8
Not a high enough priority for resources	16	11.1
Insufficient number of skilled staff	9	6.3
Attestation is handled at time of hire	10	6.9
Other (In process or handled elsewhere)	10	6.9
Insufficient amount of financial resources	7	4.9
Difficulty determining information security value	7	4.9
New Hire initial training is sufficient	7	4.9
Does not apply to our organization	1	.7

When training was conducted, the majority of respondents reported that all personnel attend (56.4%). The most commonly used methods to deliver training included: face-to-face training sessions (53.5%), email messages (52.5%), online training using

web or intranet-based access (46.5%), newsletters (28.7%), and posters and flyers (26.7%) (Table 10).

Topics covered most often included policies (72.3%), acceptable use (72.3%), password protection (71.3%), workstation security (63.4%), confidentiality (61.4%), viruses (60.4%), remote access (54.5%), information sensitivity and classification (51.5%), and bringing in software from home or inappropriate licensing (49.5%) (Table 10).

Table 10. Frequency and Percentages for Security Awareness Training Delivery Methods and Topics by Percent of Participants in Organizations Reporting Security Awareness Training Offered.

	N	%
Security Awareness Training Delivery Methods		
Face-to-face training sessions	54	53.5
Email messages	53	52.5
Online training (web or intranet-based)	47	46.5
Presentations, speakers	32	31.7
Newsletters	29	28.7
Posters, flyers	27	26.7
Videos	13	12.9
Slogans or bulletin boards	12	11.9
Monthly topic spotlight	10	9.9
CD-ROM/DVD	10	9.9
Mail stuffers	2	2.0
Security Awareness Training Topics		
Policies	73	72.3
Acceptable use	73	72.3
Password protection	72	71.3
Workstation security	64	63.4
Confidentiality	62	61.4
Viruses	61	60.4
Remote access	55	54.5
Information sensitivity and classification	52	51.5

Table 10 (cont.)

	N	%
Security Awareness Training Topics (cont.)		
Bringing in home software/licensing	50	49.5
Downloading shareware software	47	46.5
Integrity of data/information	40	39.6
Spyware	39	38.6
Incidents reporting	39	38.6
Identity theft	36	35.6
Specialized compliance (HIPPA, FERPA, etc.)	33	32.7
Risk assessment	29	28.7
Availability/Disaster recovery	26	25.7
Social engineering	26	25.7
Service pack or OS updates	17	16.8

When security awareness training was conducted, respondents reported that IS or Security staff typically conducted security awareness training (58.3%). Training sessions were primarily offered once a year (45.3%), and usually flexible enough to incorporate new issues or needs (76.6%). Although input was frequently based on experiences or incidents (53.4%), input was also solicited from end users (41.9%). The majority of respondents (72.1%) had received security awareness training within the last year, with 52.6% of them reporting training within the last six months (Table 11).

Of those respondents that report security awareness training is offered, 51.3% receive security awareness training on social engineering. Most participants concurred that management agrees on the topics (51.4%). There was no significant difference, however, by type of organizations, number of employees, or region on whether security awareness training involving social engineering was conducted.

Table 11. Frequency and Percentages for Security Awareness Training by Percent of Participants in Organizations Reporting Security Awareness Training Offered.

	N	%
Frequency of training sessions per year		
Not at all	5	6.7
Once per year	34	45.3
Twice	6	8.0
Three to five	13	17.3
Six to ten	7	9.3
Greater than 10	10	13.3
Latest security awareness training session received		
New hire training	1	1.3
Less than 6 months	41	52.6
6 months to 1 year	23	29.5
1 to 2 years	6	7.7
2 to 5 years	2	2.6
Training provider		
IS/Security staff	56	58.3
Management	27	28.1
Outsourced	12	12.5
Speakers/presenters	19	19.8
Social Engineering training offered		
Yes	41	51.3
No	29	36.3

A greater percentage of respondents report that security awareness training is not designed and tailored to different groups within the organization (46.2%) as compared to those who report training is customized (34.5%) (Table 12).

Policies

Since matrix sampling was used, respondents were assigned random sections to complete after completing the demographics and training sections. Ninety-one

Table 12. Frequency and Percentages for Security Awareness Training by Percent of Participants in Organizations Reporting Security Awareness Training Offered.

	N	%
Training customized for different organizational groups		
Yes	27	34.6
No	36	46.2
Do not know	15	19.2
Training flexibility to incorporate new issues/needs		
Yes	59	46.6
No	3	3.9
Do not know	15	19.5
Topic input solicited from end users		
Yes	31	41.9
No	24	32.4
Do not know	19	25.7
Topic input based on experiences/incidents		
Yes	39	53.4
No	11	15.1
Do not know	23	31.5
Agreement by management on topics		
Yes	38	51.4
No	2	2.7
Do not know	34	45.9

respondents completed the Policies section. Only 3.4% reported that their organization had no policies. Of the respondents answering the Policies section, the types of policies with the highest reported percentage of use were acceptable use (89.0%), email (84.6%), password (78.0%), backup and recovery (71.4%), anti-virus (70.3), software installation and licensing (67.0%), disaster recovery (58.2%), and physical security of sensitive areas (58.2%) (Table 13).

Table 13. Frequency and Percentages for Policies in Use by Percent of Participants in Organizations Completing Policy Section Questions.

	N	%
Security policies in use		
Acceptable use	81	89.0
Email	77	84.6
Password protection	71	78.0
Backup and recovery	65	71.4
Anti-Virus	64	70.3
Software installation and licensing	61	67.0
Ethics	55	60.4
Physical security (sensitive areas)	53	58.2
Disaster recovery	53	58.2
Remote access	52	57.1
Visitor control	52	57.1
Business continuity	45	49.5
Dial-in access policy	38	41.8
Email retention	39	42.9
Information sensitivity	44	48.4
Incident reporting	44	48.4
Overall information security plan	37	40.7
IS Security plan/program	30	33.0
Patch management	25	27.5
Risk assessment	24	26.4
Vendor oversight	22	24.2
Handheld policy	20	22.0
Extranet	18	19.8
Social engineering	13	14.3

One of the policies that is least used is social engineering. Only 20.5% of respondents reported that they have policies regarding social engineering (Table 14) and only 14.3% reported the social engineering policies in use.

When asked who participates in the development of information security policies, IS staff received the highest percentage (60.4%), followed by IS security personnel (34.1%), department managers (24.2%), IS steering committee (17.6%), and all

Table 14. Frequency and Percentages for Social Engineering Policies by Percent of Participants in Organizations Completing Policy Section Questions.

	N	%
Existence of social engineering policies		
Yes	18	20.5
No	37	42.0
Do not know	33	37.5

employees (6.6%). Other individual responses included records managers, internal audit, legal, data custodians committee, IT, and VP of document management.

A high percentage of respondents had read one or more security policies within the last year (83.3%) with 63.3% reporting having read them within the last six months. The majority also reported reading *all* of the security policies that apply to themselves. The percentage distribution for having read the policies within the last two years was: within the last 6 months (31.5%), six months to one year (27.0%), and one to two years (13.5%).

Policies seem to be readily available for employees with a majority reporting that policies are easily available (69.3%) or somewhat available (17.0%). Also, almost all reported that the security policies were not too restrictive (92.0%).

Compliance

Most respondents reported that they know the consequences for failing to comply with their organization’s security policies (81.7%). Consequences for failure to comply were typically included in other policies (65.4%). Most organizations also required employees to sign off or attest to: reading policies (62.5%) and attending training (62.7%).

A substantial percentage of respondents reported that there were penalties or consequences for breaches of security including social engineering (48.8%); however, 41.5% did not know if there were consequences and only 9.8% reported no consequences.

On the other hand, a relatively low percentage of respondents reported use of methods to motivate users. As a percent of total respondents, only 9.2% reported creative and diversified delivery methods, 2.3% provide incentives and rewards for compliance, 13.8% use compliance as a factor in employee evaluation, 23.1% strong security culture, and penalties for non-compliances 30.8%.

When respondents were asked what motivates them personally to comply with security policies, the top three motivators were individual motivation ranked as the highest ($M = .47$) followed by employee responsibility for information security ($M = .39$), and importance placed on information security ($M = .32$).

When asked to rate the most effective motivational strategies for compliance, similar responses were found. The top four strategies were importance placed on information security ($M = 2.25$) as the most effective, followed by employee responsibility for information security ($M = 2.26$), individual motivation ($M = 2.43$), and penalties for non-compliance ($M = 2.47$).

Auditing and Testing

Only a few respondents reported that social engineering testing is conducted in their organization (8.1%). However, although 34.7% reported social engineering testing is not conducted, a large percentage did not know if it was conducted (57.3%). Most respondents also did not know why it was not conducted (73.8%). Of the few that did

report reasons, lack of people resources (7.8%) and social engineering testing not being a high priority (8.7%) received the highest percentages.

As far as the types of social engineering tests or scenarios conducted, limited information was available. A few respondents' comments included that they were not given that information; another reported they get creative and try to simulate real-world scenarios that employees would encounter performing their duties; and another comment included physical security and access tests or helpdesk requests.

Audits were reported to be conducted by 66.1% while 10.5% did not with 23.34% reporting that they did not know if they were conducted. Respondents were also asked if penetration tests were conducted. Although 24% of respondents reported external penetration testing and 18.4% reported internal penetration testing, 63.2% reported that they did not know.

Security Awareness and User Perceptions

Respondents were asked to rate their level of agreement or disagreement with several statements regarding security awareness and its status within their organizations. The scale ranged from Strongly Disagree = 1 to Strongly Agree = 5. The highest level of agreement was found in the following statements: people are equally as important to security as technology (M = 4.40); computer/information security is an important concern to me (M = 4.30); I know who I would report a possible security breach to (M = 4.27), and I am motivated to follow security guidelines (M = 4.25). Respondents also tended to agree they would be able to recognize a security policy violation if they saw one (M = 3.78) and they would like to receive more information security training from their organization (M = 3.69).

Most disagreed with the statement that exhibiting good security behavior is rewarded (M = 2.49). Also, there was general disagreement that achievement of security awareness goals is measured or assessed (M = 2.66), effectiveness of overall security awareness program is evaluated or measured (M = 2.74), and there was assessment for continuous improvement of the security awareness or information security program (M = 2.79). Respondents also disagreed that incident response procedures were well understood.

Statements that showed little or no agreement or disagreement included security goals were clearly communicated (M = 2.96), the security message is repeated often (M = 2.98), policies were reviewed and updated regularly (M = 3.05), there was a security culture within their organization (M = 3.06), and security awareness goals are clearly identified (M = 3.15) (Table 15).

Table 15. Mean Scores for Respondents' Level of Agreement with Statements on a Scale of 1 for Strongly Disagree to 5 for Strongly Agree.

	M
People are equally important to security as technology.	4.40
Computer/information security is an important concern to me.	4.30
I know to whom I would report a security breach	4.27
I am motivated to follow security guidelines.	4.25
I would be able to recognize a security policy violation if seen.	3.78
I would like to receive more information security training from my organization	3.69
Security awareness is an ongoing focus in our organization	3.54
I know the procedure to report a security incident or breach	3.40
I understand the meaning of "social engineering."	3.35
All staff is required to sign off on reading information security policies.	3.32
Security awareness goals are clearly identified.	3.15
There is a security culture within our organization.	3.06

Table 15 (cont.)

	M
Policies are reviewed and updated regularly.	3.05
The security awareness message is repeated often	2.98
Security awareness goals are clearly communicated.	2.96
I feel empowered to make decisions involving security of information and technology	2.91
Exhibiting good security behavior is recognized.	2.89
Computer security is a concern/responsibility for IT rather than end users.	2.83
There is assessment for continuous improvement of the security awareness or information security program.	2.79
Effectiveness of overall security awareness program is evaluated or measured.	2.74
Achievement of security awareness goals is measured or assessed.	2.66
Incident response procedures are well understood.	2.62
Exhibiting good security behavior is rewarded.	2.49
Security is primarily a technical issue.	2.28

Several MANOVAs were calculated to determine whether any differences existed by type of organization, size of organization, or region on many of the security awareness and perception variables. No significant differences were found by any of the three demographic variables.

Discussion

Much progress has been accomplished in improving security awareness. This study found that 60% of organizations conduct security awareness training, almost half mandate training and of the 60% that offer training, approximately 40% track attendance at security awareness training. This statistic compares to 73% of respondents from organizations required to comply with internal control regulations in the 2005 Ernst & Young study involving executives from over 50 countries. Although a majority of

organizations offer training, 40% still do not offer security awareness training or know if they offer it.

An interesting and somewhat surprising finding is that there was no significant difference by type of organization, number of employees, or region on whether training was conducted or mandated or on whether security awareness training on social engineering was conducted. One might have thought that organizations that are more regulated or required to have internal controls in place would have had a higher percentage. There was no overwhelming reason for not offering training, although lack of management awareness, support, or commitment, the belief that end users know better, and that it is not a high enough priority for resources were mentioned more frequently. The latter reason has been cited in other research studies.

Face-to-face training, email, and web or intranet-based forms of training are still the most prevalent types of training. Topics covered included many of the traditional topics such as acceptable use, policies, passwords, workstation security, confidentiality, and viruses. Topics receiving a low percentage of coverage included important topics such as availability/disaster recovery (25.7%), incidents reporting (38.6%), downloading shareware software (46.5%) and bring in software from home/inappropriate licensing (49.5%). This is not only surprising but also an area of concern that should be given consideration by organizations. Coverage of these important topics could be increased significantly.

Results indicated that training was not typically customized for different organizational groups. Customizing or personalizing the training to show how it can benefit people in their jobs has been frequently recommended as a method that can be

used to increase the effectiveness of the training and help users incorporate what they have heard (Wilson and Hash, n. d.; Orchesky, 2003). Respondents tended to feel, however, that training was flexible to incorporate new issues and based on experiences. They also felt there was agreement by management on topics, and that input was solicited from users.

Many positive perceptions and beliefs regarding various aspects of information security were found. A high percentage view information security as important, view people as an important security component, and feel motivated to follow security guidelines. Most seem to feel comfortable being able to recognize a security violation and know the person to whom they should report any security breach.

Although respondents seem to know to whom they would report a security breach ($M = 3.78$), they did not believe that incident response procedures were well understood ($M = 2.62$). Although these professionals rated their knowledge of the procedures to report a security breach somewhat higher ($M = 3.40$), it was still far from an Agree or Strongly Agree rating. A possible reason is that only 48.4% have incident reporting policies and only 38.6% of those that offer training cover incidents reporting. There is still another 40% that do not have training.

It is very possible that incidents may go unreported because users may not understand all of the events that could be considered a breach nor clearly understand how and when to report a breach. This can represent a serious concern for organizations, because they cannot take appropriate action until an incident is reported. If organizations cannot take immediate action, then other problems also could occur as a result.

Social engineering attacks are on the increase. These types of attacks can be just as lethal for organizations as other attacks. Users within organizations and their behavior are primary targets for these attacks and therefore, deserve considerable attention and coverage in a security awareness program. In this study, social engineering was rated as one of the least offered training topics in security awareness training, and only 51.3% of the 60% that offered security awareness training offered social engineering training. Only 20.5% of respondents reported social engineering policies, and only 8.1% reported social engineering testing. This represents a high-level of concern and efforts should be initiated to ensure policies and training sessions exist on this area.

Assessment and evaluation are necessary to determine if progress or improvement in security awareness is being achieved, provide feedback to make adjustments in the program, and provide a baseline from which to evaluate the program. Survey respondents tended to disagree with any statements that said security awareness programs or goals were being assessed for continuous improvement or achieving goals. It is difficult for organizations to improve or even know whether their security awareness training and programs are effective if they do not measure it.

Measurement helps to determine if program and training objectives have been met as well as the amount of progress achieved in raising the security awareness of users. Measurement not only can find out whether the awareness program is effective, but also can help to identify any knowledge gaps and ensure the continuity and improvement of the overall security awareness program (Wulgaert, 2005).

Surveys, interviews, exams, and audits are a few of the more common assessment tools that can be used to measure progress. However, social engineering testing is another

example of a successful method that can be used to measure effectiveness of the organization's security awareness program.

Feedback obtained from these assessments can then be used to provide direction in making modifications, improvements, or additions to the program. Assessment also needs to occur periodically so that the program can additionally accommodate the changes and new security issues that arise in such a dynamic environment.

Assessment signifies an area that should be examined further in organizations in an effort to increase its use so that continual improvement and growth can occur. Improvement and growth, in turn, will allow for security awareness to be fully integrated in the organizations, assisting in the overall maturing of the information security program.

Good security behavior seems to neither be recognized nor rewarded, yet many respondents felt they were motivated to follow security guidelines either because of individual motivation and employee responsibility or penalties for noncompliance. This would seem to indicate that information security is part of everyone's job responsibility, and that rewards should not become a primary motivating factor.

Other areas where mean scores were very average and could potentially be improved were updating policies on a regular basis, identifying and communicating the security awareness goals and message, repeating the security message often, and creating a security culture. Management awareness, commitment, and support were a few of the more common reasons given for security awareness training not being conducted. If management commitment is increased, and the security awareness goals and message are

communicated and communicated often, then progress and improvement can be made in creating a security culture.

Audits are also conducted by a majority of the organizations (66.1%) as compared to 87% found in the 2005 CSI/FBI Computer Crime and Security Survey (Gordon et al., 2006). However, 23.34% did not know if audits were conducted. It was difficult to determine the extent of internal or external penetration testing as 63.2% reported that they did not know. The large percentage of respondents not knowing this information could be attributed to testing being a concern and responsibility of IS departments and staff rather than other individuals responsible for the management of information within the organization.

Implications

Although much progress has been achieved in improving the status of security awareness in organizations, there is still some work to be done to achieve maturity across the board in these programs. Although 60% offer security awareness training, there is still a significant 40% that do not. Organizations that do not have such a program need to seriously look at beginning a security awareness program to strengthen this aspect of their security defense system and protect their information resources. Technology alone is not a comprehensive solution. Involving top management and getting their support is essential in building a strong security awareness program that employees will take seriously.

Security awareness training needs a foundation of policies. Although many types of policies are in use, there needs to be more development of policies for incidents reporting, availability/disaster recovery, and social engineering. These policies are

extremely important and should be included within organizations' information security program. Once they are developed, it is crucial that employees receive training on these topics. Most respondents indicated that policies are available and they have read policies recently. This is a positive finding.

Equally positive is that most respondents viewed information security as important, recognized people as an important security component, realized they have a responsibility to help protect information resources, and felt an individual sense of motivation to follow security guidelines. It also appeared that organizations have penalties for noncompliance, which seemed to serve as an additional motivator.

Social engineering is an area that needs attention by more organizations. Although it can represent as lethal a threat as other types of attacks, it is receiving very limited attention within organizations. Social engineering policies and training need to be developed and implemented. Social engineering testing should also be conducted to assess the effectiveness of the security awareness program and specifically social engineering awareness.

Assessment of security awareness programs and training also needs strengthening in organizations. Security awareness goals first need to be clearly communicated and the security awareness message repeated often. Assessment is necessary to measure progress in achieving goals and to obtain necessary feedback that can be used to make modifications and improve the security awareness program.

Organizations should be recognized for the achievements and progress accomplished in building their security awareness programs. By implementing some of the changes discussed above, they can increase coverage of components found in more

formalized security awareness programs, achieve higher levels of security awareness maturity, and a stronger security culture.

CHAPTER V

CONCLUSIONS AND RECOMMENDATIONS

This chapter summarizes the colleges of business study from chapter three and the organizational study from chapter four. Implications for education, organizations, and research are presented followed by overall conclusions and recommendations.

Security Awareness in Colleges of Business

This study investigated the extent to which colleges and universities are offering security awareness topics as part of a student's coursework or daily activities in colleges of business. The study examined whether or not security awareness training was conducted, and if it was, the training methods that were used. The study also examined coursework to learn what topics were being covered, how often, and in what departmental areas. Faculty perceptions and level of importance given to security awareness was then explored.

The researcher constructed a survey instrument covering demographics, security awareness training, information security awareness in coursework, and security awareness training and education perceptions and beliefs. Data was collected from 85 subjects across multiple departments. Standard statistical analyses (including descriptive statistics, MANOVAs, and Pearson correlation calculations) were run to answer two research questions:

1. What is the status of security awareness education in AACSB-accredited colleges of business?
2. What differences exist between selected demographic variables and selected security awareness education variables within AACSB colleges of business?

Results found that the majority of survey participants reported that their colleges of business do not conduct security awareness training for faculty or students. When security awareness training was conducted, approximately one-third mandated training and tracked attendance. Email messages and face to face training were the most common delivery formats. Integration of IT security and awareness topics was low with a majority of respondents reporting less than 25% integration or no integration. Information security was a concern to most faculty members and a majority felt they should receive more information security and awareness training. Faculty tended to feel that graduating students were not well prepared to meet the security challenges in today's work world. Although a majority of faculty members view security awareness knowledge as important in the business curricula, about one third did not. However, about 30% would like to increase coverage of these topics within their courses.

Security Awareness in Organizations

The study of security awareness in organizations focused on security awareness training, IT-related policies, and the use of social engineering testing. User perceptions were also explored. A survey instrument was constructed by the researcher to examine demographics, training, policies, compliance, auditing and testing, and user perceptions related to information security awareness. Data was gathered from 144 participants involved in records and information management. Standard statistical analyses including

descriptive statistics, MANOVAs, and Pearson correlation calculations, were conducted to answer the following research questions:

1. What was the status of security awareness training, IT-related policies, and the use of social engineering testing in business organizations?
2. What differences exist between selected demographic variables (type of organization, number of employees, United States geographic region, and department) and selected user perception and security awareness variables?
3. Was the perception of security among small organizations different than large organizations?

Much progress in improving security awareness within organizations has been achieved. Most are offering training, making their policies readily available, and conducting audits. The majority of respondents (60%) reported that their organizations offer security awareness training, and almost half of them mandate the training. A significant percentage of organizations that do not offer security awareness training, however, still exists. There was no significant difference by type of organization on whether training was offered which may be somewhat surprising. However, no separate delineation was constructed to categorize organizations by those required to comply with internal control regulations and those that are not required. Face-to-face training, email, and intranet or web-based training were reported to be the most common delivery methods of training, but no customization of training for different groups within the organization was prevalent.

Although many security awareness topics were reported by a high percentage of respondents, some very important security awareness topics such as availability/disaster

recovery, incidents reporting, downloading shareware software, and bringing in software from home/inappropriate licensing received much lower percentages.

Other areas of the study that warrant additional attention include social engineering, incident response, and assessment of security awareness programs, goals, and training. Social engineering training was a topic that was located toward the bottom of the list of training topics offered by percentage of respondents reporting it offered. A low percentage of respondents also reported social engineering policies and social engineering testing. Overall, respondents did not feel that incident response procedures were well understood. Only one third of those that report security awareness training reported incident reporting as a training topic. Survey respondents also tended to disagree with statements reflecting that security awareness programs or goals were being assessed for achieving goals or for continuous improvement.

Many positive findings were also discovered. Respondents reported that policies were readily available and that they had read them within the last six months or least within the last year. The majority of respondents also indicated that they follow security guidelines and are motivated by an individual sense of responsibility.

Implications for Colleges of Business Faculty

This study suggests that colleges of business faculty may want to consider integrating and increasing their coverage of security awareness topics in business courses. Only 20% of faculty respondents believed that students were prepared to meet the security challenges of today's business world.

The majority of organizations now offer security awareness training, and many have achieved much progress in improving their security awareness programs, partly in

response to legislation that requires compliance with internal control regulations. Since colleges of business prepare their future graduates for careers in business, the curriculum should also reflect the importance of security awareness and selected information security topics.

Almost one third of those surveyed would like to increase coverage of information security and awareness topics within their courses. With this level of interest, faculty could start mapping security awareness and information security topics currently being offered to the courses in which they are offered. They could also begin discussion with other faculty to learn what they are offering and talk about any potential interdisciplinary offerings or collaborations. Since Information Systems departments are considered a primary deliverer of this subject, they may want to initiate the discussions with other departments or at least be involved significantly in the discussions. Many opportunities exist for collaboration between departments. Just as multiple departments, multiple job roles, and management within organizations are involved with various aspects of information security, the same could be applied to the academic instructional arena. At a minimum, everyone (whether students or employees) needs basic security awareness literacy, because protection of information resources is every user's responsibility in the organization. In addition, important topics such as risk assessment, incident reporting, policy development, auditing, and testing are relevant topics that could be addressed in various courses in multiple ways.

Discussions between faculty regarding security awareness integration within the business curricula and the addition of security awareness training opportunities also may

help some of the one-third of respondents that do not view security awareness topics as important.

Since the majority of colleges of business at the present time do not offer security awareness training for faculty or students, they could begin on a small scale and build their program over time. Faculty respondents also believed that faculty and students should receive more information security and awareness training. Because there is frequent competition for financial and people resources, colleges could begin integrating security awareness training with cost affordable methods including electronic delivery such as email, web-based or intranet-based training, or newsletters. Other signage could also be used to keep the message in focus without adding significant cost.

The statistical data also supports the notion that security awareness training and education tend to contribute to people's positive perception of security preparedness. Relationships in this study showed that participants who believed there was a security culture within their college of business came from colleges of business where security awareness training was conducted, tended to believe that students' level of security preparedness was higher, and their rating of security coverage and importance in the business curriculum was higher. These relationships support the need for training and education within the business curricula to help faculty and students understand the importance of information security and awareness, and help graduate students that are better prepared to meet the security challenges of today's business world by being equipped with many of the security awareness skills that organizations need in their employees and future employees.

Implications for Organizations

Organizations have achieved much progress in developing policies and offering security awareness training. Respondents in this study reported that policies are readily available and not too restrictive. A variety of topics are being covered, and users are reading policies. Organizations should be commended for their positive efforts and outcomes in these areas.

A few areas that have the potential for continued improvement, however, were found. More development of policies for incident reporting, availability/disaster recovery, and social engineering are needed. Once the policies have been developed, security awareness training needs to be conducted on these topics. Since respondents believed that the procedures for incident reporting were not well understood, training not only would help to clarify and explain the procedures, but also help to ensure that incidents are reported and reported promptly. Proper incident reporting is critical for organizations, so that appropriate action can be taken quickly.

Social engineering can present as lethal a threat as other types of attacks, but many organizations have not yet incorporated social engineering policies or training into their information security program. Respondents reported low percentages of social engineering policies, training, and testing in use. Since social engineering targets unsuspecting users in organizations, users are a prime target for these attacks especially if they are not trained in how to recognize a potential social engineering attempt or attack, or are not clear what information can or cannot be divulged and to whom.

Discrepancies in two sets of responses to social engineering questions were noticed by the researcher which could possibly be attributed to confusion by respondents

as to what social engineering fully entails, even though a general definition was given. Developing the policies, offering the training, and following up with social engineering testing (to evaluate the effectiveness of the training) will strengthen and solidify the defenses against this potential vulnerability.

Organizations also can continue to grow and improve their security programs by incorporating more assessment into their information security awareness program. Assessment and the corresponding feedback received can provide the valuable information necessary to make modifications or additions that will strengthen the security awareness program and its effectiveness, leading to a more formalized and mature security awareness program.

Implications for Researchers

Several questions arose as a result of these studies. Since information security is part of a larger dynamic environment, opportunities will exist for research far into the future.

Future research could examine different types of organizations with respect to information security awareness models to determine the level of maturity within different types of organizations. Research could also examine the number of social engineering types of attacks and losses caused as a result. Research also could examine what organizations are doing with information security awareness for new advanced technologies such as VoIP (Voice over Internet Protocol). Another question that could be answered is: how well is the security awareness message being communicated across all levels of the organization--would you get the same answer by all users? Research could

be conducted to see if the same or different results are obtained with other population samples or even within organizations including different types and levels of employees.

Colleges of business's opportunities for research could explore perceptions of recent graduates and employers regarding their security awareness preparedness. Research could also examine the security awareness knowledge and skills employers would like to see in new graduates. Research could examine whether colleges of business offer a required course in security awareness or explore any interdisciplinary courses being offered related to security awareness. Research could also explore types of courses being offered that include security awareness and the topics and skills covered in them.

Conclusions and Recommendations

Information security and awareness will be important concerns well into the future. Organizations and education both need to assess their security awareness training and education programs to ensure that goals and objectives are being met. Assessment is necessary for program improvement, growth, and maturity. Programs need to stay abreast of new technologies and the associated information security issues so that appropriate coursework or security awareness programs can incorporate those new topics. Higher education and organizations should communicate with each other regularly so that college curriculums can teach the knowledge and skills sets organizations need, thereby preparing students adequately for future jobs and also benefiting the organizations that hire them. Effective communication of policies and security awareness topics within organizations is essential so that all users across all levels will have the same knowledge regarding information security awareness, policies, and procedures. Keeping the message in constant focus, getting top management support, and creating a security culture will

help to strengthen an organization's security chain. Assessment and continuous improvement will facilitate growth and maturity of security awareness program into the future.

APPENDICES

Appendix A
Security Awareness in Colleges of Business Survey Instrument

Demographic Information

1. What is your department?
 - Accounting
 - Finance
 - Information Systems
 - Marketing
 - Political Science and/or Public Administration
 - Economics
 - Management
 - Other: _____

2. What is the number of students enrolled in your college of business?
 - Less than 1,000
 - 1,001-1,500
 - 1,501-2000
 - 2,001-2,500
 - 2,501-3000
 - 3,001-4000
 - 4,001-5000
 - Greater than 5,000

3. In what state do you work?
Alabama

4. What is the approximate number of full-time faculty (tenure-track and non-tenure track) in your *college of business*?
0

5. What is the approximate number of full-time faculty (tenure-track and non-tenure track) in your *department*?
0

6. What percent of full-time faculty in your department are tenure-track?
 - Equal to or greater than 90%
 - 70-89%
 - 50-69%
 - Less than 50%

7. Does your college of business have its own Information Technology personnel and support services?
 - Yes
 - No

8. Rate your college of business's use of technology.
 - High (Cutting edge)
 - Above Average (Up-to-date)
 - Average
 - Below Average
 - Very Limited (Outdated)

Next Page

**Data for this page will be saved
when you click Next Page.**

Information Security Awareness Training

Security Awareness Training is defined as presenting or giving information to individuals regarding various security topics to help protect the safety and privacy of information within an organization and for the purpose of this study excludes a student's regular coursework. Training can include one or more of the following formats: face-to-face training sessions, online training, CD-ROM/DVD-ROM, newsletters, posters, flyers, videos, email messages, slogans, bulletin boards, presentations, speakers, mail stuffers, monthly topics spotlights, or other similar formats.

9. Is security awareness training conducted in your college of business for *faculty*?
- Yes
 No
10. Is security awareness training conducted in your college for *students*?
- Yes
 No

If security awareness training is not conducted for either groups in 11. your college of business, why is it not conducted? (Check all that apply)

- Insufficient number of skilled staff
 Insufficient amount of financial resources
 Not a high enough priority for resources
 Difficulty in determining the value of information security
 Does not apply to our organization
 Lack of management support/commitment
 Lack of awareness by management
 Other:

Not applicable

Next Page

**Data for this page will be saved
when you click Next Page.**

If security awareness training is *not* conducted within your college of business, skip to the next section by pressing skip--*Security Awareness Education in Coursework*, Question 19.

Skip

12. Is security awareness training mandatory for faculty and staff?
- Yes
 - No
 - Not applicable
13. Is security awareness training mandatory for students?
- Yes
 - No
 - Not applicable
14. Who attends security awareness training? (Check all that apply)
- All personnel
 - Administration
 - Faculty
 - Information Systems (IS) staff
 - Administrative support
 - Students
 - Other:
 - Not applicable
15. Is attendance at security awareness training maintained?
- Yes
 - No
 - Not applicable
16. What methods are utilized to deliver security awareness training? (Check all that apply)
- Face-to-face training sessions
 - Online training (using web or intranet-based access)
 - CD-ROM or DVD-ROM
 - Newsletters
 - Posters, flyers
 - Videos
 - Email messages
 - Display of catchy slogans or bulletin boards

- Presentations, speakers
- Mail stuffers
- Monthly topic spotlight
- Other:

Not applicable

17. What topics are covered in IT Security Awareness training? (Check all that apply)

- Acceptable use
- Viruses
- Password protection
- Workstation security
- Email security
- Internet security
- Confidentiality
- Spyware
- Download shareware software
- Bringing in software from home (inappropriate licensing)
- Remote access
- Information sensitivity and classification
- Social engineering
- Service pack or Operating System updates
- Incidence reporting
- Risk assessment
- Specialized Security (ex: HIPAA, FERPA, etc.)
- Identity theft
- Other:

Not applicable

18. Who is responsible for training? (Check all that apply)

- IS Staff/Security staff
- Management
- Outsourced
- Speakers/Presenters
- Other:
- Do not know
- Not applicable

Next Page

**Data for this page will be saved
when you click Next Page.**

Security Awareness Education in Coursework

19. Which IT Security and Security Awareness topics are integrated into coursework of your business core courses (courses required for all business students) offered by your department? (Check all that apply)

- Acceptable use
 - Viruses
 - Password protection
 - Workstation security
 - Email security
 - Internet security/Staying safe online
 - Confidentiality
 - Spyware
 - Downloading shareware software
 - Bringing in software from home (inappropriate licensing)
 - Remote access
 - Information sensitivity and classification
 - Social engineering
 - Service pack or operating system updates
 - Incidence reporting
 - Risk assessment
 - Special security (ex: HIPAA, FERPA, etc.)
 - Identity theft
 - Internal controls--process controls
 - IT governance
 - IT/Security policy development
 - IT Security controls--technical (firewalls, intrusion detection, access controls, etc.)
 - Top management's role in development of a security program
 - Security threats
 - IT Security controls--human safeguards
 - IT Security controls--administrative/data
 - Other:
- No security awareness topics are integrated

20. IT Security and Information Security Awareness topics are integrated into approximately what percent of courses in your department?

- 90-100%
- 75-89%
- 50-74%
- 25-49%
- Less than 25%
- 0%

21. In your estimation, how well prepared are your graduating students in terms of Information Security Awareness topics?

- Extremely well prepared
- Moderately well prepared
- Somewhat prepared
- Not well prepared

22. Rate the importance of Information Security and Awareness knowledge in the business student's curriculum.

- Extremely important
- Moderately important
- Important
- Not very important
- Not needed

Next Page

**Data for this page will be saved
when you click Next Page.**

Security Awareness Education in Coursework (continued)

Answer questions 23-26 using the scale below.

- Extensive = integrated into most units
- Significant = integrated into approximately half of the units covered
- Moderate = integrated into a few units
- Special unit = one unit or chapter
- Not covered

	Extensive	Significant	Moderate	Special Unit	Not Covered
23. Generally, rate the amount of coverage of information security and awareness topics in elective courses offered by your department.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
24. Generally, rate the amount of coverage of information security and awareness topics in courses that are part of the major offered by your department	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
25. Generally, rate the amount of coverage of information security and awareness topics in courses offered by other departments in the college of business.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
26. Generally, rate the amount of coverage of information security and awareness topics in courses that are offered in departments outside the college of business.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>

Next Page

**Data for this page will be saved
when you click Next Page.**

Security Awareness Training and Education Perceptions and Beliefs

Rate your level of agreement with the following statements.

	Strongly Agree	Agree	Do Not Agree or Disagree	Disagree	Strongly Disagree	Not Applicable
27. Our department would like to increase the coverage of information security and awareness topics within our courses.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
28. Information Security and Awareness topics should be only taught by the Information Systems department faculty.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
29. There is a security culture or shared beliefs and behaviors, regarding information security within your college.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
30. Information security and awareness should be integrated into most business courses.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
31. Information security and awareness should be taught <i>only</i> in Information Systems (IS) courses.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
32. Information security and awareness should be taught <i>primarily</i> in IS courses.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
33. Computer/information security is an important concern to faculty.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
34. Security is primarily a technical issue.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
35. People are equally as important to security as technology.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
36. Faculty should receive more training on information security and awareness.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
37. Students should receive more education on information security and awareness.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
38. Graduating students are prepared to meet the security challenges in today's work world.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Click to be done!

**Thank you for participating in the Security
Awareness survey.**

Your time and valuable input is greatly appreciated. Results obtained from this research not only will help to increase understanding of where colleges of business are in terms of security awareness maturity and integration of information security related content into the curriculum by various demographics, but also will help colleges of business and faculty benchmark with peers or statistically similar institutions.

If you would like a copy of the results of this study, you can send a self-addressed, stamped envelope to: Glenda Rotvold--Security Awareness Study Results, Information Systems and Business Education Dept., University of North Dakota, Box 8363, Grand Forks, ND 58202

Appendix B
Security Awareness in Organizations Survey Instrument

Demographic Information

1. Classify your type of organization.
 - Healthcare
 - Banking
 - Financial Services (other than banking)
 - Manufacturing
 - Service (other than listed categories)
 - Education
 - Accounting
 - Consultant
 - Government (Federal, State, Local)
 - Energy and Utilities
 - Legal
 - Archives
 - Merchandising/Retail
 - High Tech
 - Other: _____

2. What is the approximate number of employees in your organization?
 - 1-99
 - 100-499
 - 500-999
 - 1,000-2,499
 - 2,500-4,999
 - 5,000-9,999
 - 10,000-19,999
 - 20,000-50,000
 - Greater than 50,000

3. In what state are you located?
Choose a State

4. In what department do you work?

- Do your job duties or responsibilities involve working with
5. Information Technology/Information Systems security, policies, or user training?
 - Yes
 - No

6. Is your job a management position within the organization?
 - Yes
 - No

Next Page

**Data for this page will be saved
when you click Next Page.**

Training

Social engineering is defined as *attempts to get people to reveal information or act in a manner that would result in unauthorized access to, use of, or disclosure of an information system, network, or data.*

7. Is security awareness training conducted in your organization?
- Yes
 - No
 - Do not know

8. If security awareness training is not conducted in your organization, why is it not conducted? (Check all that apply)
- Insufficient number of skilled staff
 - Insufficient amount of financial resources
 - Not a high enough priority for resources
 - Difficulty in determining the value of information security
 - Does not apply to our organization
 - Lack of management support/commitment
 - Lack of awareness by management
 - Believe end users are skilled, know how to use a computer, or know better
 - "New Hire" initial training is sufficient
 - Attestation to appropriate IT-related policies is handled at time of hire
 - Other: _____

9. Is security awareness training mandatory?
- Yes
 - No
 - Do not know

If the answer to question #7 is "no," (Is security awareness training conducted...), click to continue to question #24.

10. Who attends security awareness training? (Check all that apply)
- Administrative support
 - All personnel
 - IS Staff
 - Management
 - Other: _____

11. Is attendance at security awareness training tracked?
- Yes
 - No
 - Do not know
12. What methods are utilized to deliver security awareness training? (Check all that apply)
- Face to face training sessions
 - Online training (using web or intranet-based access)
 - CD-ROM or DVD
 - Newsletters
 - Posters, flyers
 - Videos
 - Email messages
 - Display of catchy slogans or bulletin boards
 - Presentations, speakers
 - Mail stuffers
 - Monthly topic spotlight
 - Other: _____
13. What topics are covered in IT Security Awareness training? (Check all that apply)
- Acceptable use (examples: email, Internet, workstations, all IS resources)
 - Policies
 - Viruses
 - Password protection
 - Workstation security
 - Confidentiality
 - Integrity of data/information
 - Availability/Disaster Recovery (examples: user file backup, business continuity, how to respond to disaster/incident)
 - Spyware
 - Downloading shareware software
 - Bringing in software from home (inappropriate licensing)
 - Remote access
 - Information sensitivity and classification
 - Social engineering
 - Service pack or OS updates
 - Incidence reporting
 - Risk assessment
 - Specialized compliance (examples: HIPAA, FERPA, etc.)
 - Identity theft
 - Other: _____

[Next Page](#)

**Data for this page will be saved
when you click Next Page.**

Training (continued)

14. Is training designed and tailored to different groups within the organization?
- Yes
 - No
 - Do not know
15. When is the last time you received security awareness training from your organization (either face-to-face or online format)?
- Less than 6 months
 - Between 6 months to 1 year
 - From 1 to 2 years ago
 - Between 2 and 5 years ago
 - More than 5 years ago
 - New hire training included security awareness
 - The organization does not conduct security awareness training
 - Do not know
16. How often are training sessions offered per year?
- Not at all
 - Once per year
 - Twice
 - Three to five
 - Six to ten
 - Greater than 10
17. Is training flexible enough to incorporate new issues or needs?
- Yes
 - No
 - Do not know
18. Is input for topics solicited from end users?
- Yes
 - No
 - Do not know
19. Is input for topics based on experiences/incidents?
- Yes
 - No
 - Do not know

20. Is there agreement by management on topics?

- Yes
- No
- Do not know

21. Who determines training content? (Please describe)

22. Who provides the training? (Check all that apply)

- IS/Security staff
- Management
- Outsourced
- Speakers/presenters

- Other:

Social engineering is defined as *attempts to get people to reveal information or act in a manner that would result in unauthorized access to, use of, or disclosure of an information system, network, or data.*

23. Do you receive security awareness training regarding social engineering?

- Yes
- No
- Do not know

Next Page

**Data for this page will be saved
when you click Next Page.**

Policies

24. What security policies are in use? (Check all that apply)
- Acceptable use (Internet, workstations, etc.)
 - Anti-Virus policy
 - Email policy
 - Dial-in access policy
 - Email retention policy
 - Ethics policy
 - Extranet policy
 - Information sensitivity policy
 - Remote access policy
 - Password protection policy
 - Incidence reporting policy
 - Risk assessment policy
 - Overall Information Security Plan or Program
 - IS Security Plan or Program
 - Physical security (of sensitive computer areas and/or other sensitive areas)
 - Vendor oversight
 - Visitor control
 - Handheld policy
 - Patch management
 - Backup and recovery
 - Disaster recovery
 - Business continuity
 - Social engineering policy
 - Software installation and licensing
 - Do not know
25. Who participates in the development of information security policies? (Check all that apply)
- Top management
 - IS staff
 - All employees
 - Department managers
 - IS steering committee
 - IS security personnel
 - Other:
 - Do not know

26. When in the last time you read *any* of your organization's security policies?
- Less than 6 months
 - Between 6 months to 1 year
 - 1 to 2 years ago
 - Between 2 and 5 years ago
 - More than 5 years ago
 - I have never read any security policies
 - The organization does not have security policies
 - Do not know
27. Indicate the length of time since you have read *all* of your organization's security policies that *apply to you*?
- Less than 6 months
 - Between 6 months to 1 year
 - 1 to 2 years ago
 - Between 2 and 5 years ago
 - More than 5 years ago
 - I have never read any security policies
 - The organization does not have security policies
 - Do not know
28. Rate how available your organization's security policies are to you.
- Easily available (possess copies, get emails, have intranet)
 - Somewhat available (can ask HR for policies)
 - Not easily available (do not know who to ask)
 - My organization does not have policies
29. Do you have policies regarding social engineering?
- Yes
 - No
 - Do not know
30. In your opinion, are your organization's security policies are too restrictive?
- Yes, too restrictive
 - No, not too restrictive
 - My organization does not have policies

Next Page

**Data for this page will be saved
when you click Next Page.**

Compliance

31. Do you know the consequences for failing to comply with your organization's security policies?
- Yes
 - No
 - My organization does not have policies
32. Are the consequences for failing to comply with your organization's security policies a separate policy?
- Yes, it is a separate policy
 - No, it is included as a statement within another policy (ex: "violation of this policy can be up to and including termination")
 - No, consequences are not stated in any policy
 - No, there are no consequences
 - Do not know

 - Other:
 - Not applicable
33. Are employees required to sign off or attest to:
- | | |
|--------------------|--|
| Reading policies | <input type="radio"/> Yes <input type="radio"/> No |
| Attending training | <input type="radio"/> Yes <input type="radio"/> No |
34. Are there penalties or consequences (monetary, disciplinary, etc.) for breaches of security including social engineering?
- Yes
 - No
 - Do not know
35. What methods are used to motivate end users? (Check all that apply)
- Creative and diversified delivery methods
 - Incentives and rewards for compliance
 - Factor in employee evaluation
 - Strong security culture (importance placed on security)
 - Penalties/consequences for non-compliance
 - Other:

36. What motivates you to comply with security policies? (Check all that apply)

- Individual motivation
- Pleasant/friendly work environment
- Frequent communication between management and non-management
- Penalties for non-compliance
- Importance placed on information security
- Peer pressure from others who follow procedures
- Employee responsibility for information security
- Continual focus on security

37. What are the most effective motivational strategies for compliance? Rate the motivational strategies in order of most effective with a 1 being very effective to 10 being least effective.

- 1 Individual motivation
- 1 Pleasant/friendly work environment
- 1 Frequent communication between management and non-management
- 1 Penalties for non-compliance
- 1 Importance placed on information security
- 1 Peer pressure from others who follow procedures
- 1 Employee responsibility for information security
- 1 Continual focus on security

38. I follow safe security practices.

- All the time
- Frequently
- Sometimes
- Rarely

39. If requested to whom would you give your network password? (Check all that apply)

- Your direct supervisor
- Help Desk support
- Chief security officer
- The network or system administrator
- A co-worker
- An internal auditor
- None of the above

Next Page

**Data for this page will be saved
when you click Next Page.**

Auditing and Testing

40. Are social engineering tests conducted in your organization?
- Yes
 - No
 - Do not know
41. If social engineering tests are not conducted, what is the primary reason?
- Lack of management support
 - Not a high enough priority
 - Lack of people resources
 - Lack of financial resources
 - Does not apply to our organization
 - Do not know
 - Other: _____
42. Are audits conducted?
- Yes
 - No
 - Do not know
43. Are penetration tests ("ethical hacking") conducted? (Check all that apply)
- Yes, external penetration tests are conducted
 - Yes, internal penetration tests are conducted
 - No penetration tests are conducted
 - Do not know
44. If social engineering testing is conducted, briefly explain what type:
- _____
45. If social engineering testing is conducted, how many employees are

1

Next Page

**Data for this page will be saved
when you click Next Page.**

Security Awareness and User Perceptions

Rate your level of agreement with the following statements.

	Strongly Agree	Agree	Do Not Agree or Disagree	Disagree	Strongly Disagree	Not Applicable
46. Security awareness is an ongoing focus in our organization.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
47. Security awareness goals are clearly identified.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
48. Security awareness goals are clearly communicated.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
49. The security awareness message is repeated often.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
50. I understand the meaning of "social engineering."	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
51. I am motivated to follow security guidelines.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
52. I know who I would report a possible security breach to.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
53. Exhibiting good security behavior is recognized.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
54. Exhibiting good security behavior is rewarded.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
55. Incident response procedures are well understood.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
56. There is a security culture, or shared beliefs and behavior regarding security, within our organization.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
57. Computer security is a concern/responsibility for IT and technical staff rather than end users.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
58. All staff are required to sign off on reading information security policies.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
59. I feel empowered to make decisions involving the security of information and technology.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
60. I would be able to recognize a security policy violation if I saw one.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
61. I know the procedure to report a security incident or breach.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
62. I would like to receive more information security training from my organization	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
63. Rate your level of agreement: Security is primarily a technical issue.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
64. Rate your level of agreement: People are equally as important to security as technology.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
65. Computer/information security is an important concern to me.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
66. Achievement of security awareness goals is measured (assessed).	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
67. Effectiveness of overall security awareness program is evaluated or measured.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
68. There is assessment for continuous improvement of the security awareness or information security program.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
69. Policies are reviewed and updated regularly.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Save and Finish!

**Data for this page will be saved
when you click Next Page.**

Thank you for participating in the Security Awareness survey.

Your time and valuable input is greatly appreciated. Results obtained from this research will provide useful information that can be used to make further progress toward improving the state of security awareness in various types of organizations. Statistical data not only may help to increase understanding of where organizations are in terms of security awareness maturity, but also may help organizations to benchmark and compare with their peers or statistically similar organizations. Organizations also can use information obtained to develop, improve, and implement various security awareness program components in their respective organizations.

If you would like a copy of the results of this study, you can send a self-addressed stamped envelope to: Glenda Rotvold –Organization Security Awareness Study Results, Information Systems and Business Education Dept., University of North Dakota, Box 8363, Grand Forks, ND 58202.

REFERENCES

- Aytes, K. & Connolly, T. (2004). Computer Security and Risky Computing Practices: A Rational Choice Perspective. [Electronic version]. *Journal of Organizational and End User Computing*, 16(3), pp. 22-40.
- Caruso, J. (2003, September). *Information Technology Security: Governance, Strategy, and Practice in Higher Education Key Findings*. Retrieved January 5, 2007, from <http://www.educause.edu/ir/library/pdf/ERS0305/ekf0305.pdf>
- Caruso, J. (2006, October). *Safeguarding the Tower: IT Security in Higher Education 2006 Key Findings*. Retrieved January 5, 2007 from http://www.educause.edu/ir/library/pdf/ecar_so/ers/ers0606/Ekf0606.pdf
- Cormack, A. (2001). Do We Need a Security Culture? *VINE*, 31(2), pp. 8-10.
- Damle, Pramod (2002). Social Engineering: A Tip of the Iceberg. *Information Systems Control Journal, Volume 2*, Retrieved from <http://www.isaca.org/Template.cfm?Section=Archives&CONTENTID=17032&TEMPLATE=/ContentManagement/ContentDisplay.cfm>
- Desman, M. (2003). The Ten Commandments of Information Security Awareness Training. [Electronic version]. *Information Systems Security* 11(6), pp. 39-44.
- Dewey, B., DeBlois, P., & 2006 EDUCAUSE Current Issues Committee. (2006). Top-10 IT Issues, 2006. *EDUCAUSE Review*, 41(3), pp. 58-79.

- Ernst & Young. (2004). *Global Information Security Survey 2004*. Retrieved from [http://www.ey.com/global/download.nsf/UK%20/Survey_-_Global_Information_Security_04/\\$file/EY_GISS_%202004_EYG.pdf](http://www.ey.com/global/download.nsf/UK%20/Survey_-_Global_Information_Security_04/$file/EY_GISS_%202004_EYG.pdf)
- Ernst & Young (2005). *Global Information Security Survey 2005 Report on Widening the Gap*. Retrieved from [http://www.ey.com/global/download.nsf/International/Global_Information_Security_Survey_2005/\\$file/EY_Global_Information_Security_survey_2005.pdf](http://www.ey.com/global/download.nsf/International/Global_Information_Security_Survey_2005/$file/EY_Global_Information_Security_survey_2005.pdf)
- Ernst & Young. (2006). *Achieving Success in a Globalized World Is Your Way Secure? 2006 Global Information Security Survey*. Retrieved from [http://www.ey.com/global/download.nsf/International/TSRS_-_GISS_2006/\\$file/EY_GISS2006.pdf](http://www.ey.com/global/download.nsf/International/TSRS_-_GISS_2006/$file/EY_GISS2006.pdf)
- Gordon, L., Loeb, M., Lucyshyn, W., & Richardson, R. (2005). 2005 CSI/FBI Computer Crime and Security Survey. *Computer Security Institute*. Retrieved from http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2005.pdf.
- Gordon, L., Loeb, M., Lucyshyn, W., & Richardson, R. (2006). 2006 CSI/FBI Computer Crime and Security Survey. *Computer Security Institute*. Retrieved from http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2006.pdf.
- Granger, Sarah. (2002). Social Engineering Fundamentals, Part II: Combat Strategies, <http://www.securityfocus.com/infocus/1533>, Retrieved July 21, 2006.
- Hansche, S., Beri, J., & Hare, C. (2004). *Official (ISC)²® guide to the CISSP Exam*. Boca Raton: Auerbach Publications.

- Hentea, M. (2005, June 17). *A Perspective on Achieving Information Security Awareness*. Paper presented at the 2005 Informing Science + Information Technology Education Conference. Retrieved January 8, 2007, from <http://proceedings.informingscience.org/InSITE2005/I14f89Hent.pdf>
- Im, G., & Baskerville, R. (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), pp. 68-79.
- ISC Internet Domain Survey, January 2006. Retrieved August 25, 2006, from <http://www.isc.org/ops/ds/reports/2006-01/>
- Katz, R. (2006, December). *The ECAR Study of Undergraduate Students and Information Technology, 2006 Key Findings*. Retrieved January 5, 2007, from http://www.educause.edu/ir/library/pdf/ecar_so/ers/ers0606/Ekf0606.pdf
- Komiega, K. (2001). Hacker tactics prey on gullible, curious. *Search Security*. Retrieved January 31, 2006, from http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci537875_00.html
- Lee, C. (1995). A study of financial institutions' information security: Factors that influence employees' willingness to adhere to information security procedures. D.B.A. dissertation, Golden Gate University, San Francisco, California. Retrieved April 9, 2007, from ProQuest Digital Dissertations database. (Publication, No. AAT 9610740).
- Mitnick, K., & Simon, W. (2002). *The Art of Deception: Controlling the Human Element of Security*. Indianapolis: Wiley Publishing, Inc.

National Institute of Standards and Technology (2006). FISMA Implementation The Strategy, Challenges, and Roadmap Ahead. Computer Security Division, Information Technology Laboratory. Retrieved January 4, 2007.

<http://csrc.nist.gov/sec-cert/PPT/fisma.pdf>.

Orgill, G., Romney, G., Bailey, M., & ORgill, P. (2004). *The Urgency for Effective User Privacy-education to Counter Social Engineering Attacks on Secure Computer Systems*. SIGITE '04, October 28-30, 2004, Salt Lake City, Utah. Copyright 2004 ACM.

Orshesky, C. (2003). Beyond Technology—The Human Factor in Business Systems. *Journal of Business Strategy*, 24(4), pp. 43-47.

Panko, R. (2004). *Corporate Computer and Network Security*. Upper Saddle River: Prentice Hall.

Peikari, C., & Chuvakin, A. (2004). *Security Warrior*. Sebastopol: O'Reilly Media, Inc.

Peltier, T. (2005). Implementing an Information Security Awareness Program. *Information Systems Security*, 14(2), pp. 37-48.

Perez, M., Berry, R., & Hollman, C. (2003). Information Technology Security Awareness in Academia: An Initial Assessment. *Issues in Information Systems*. Volume 4. Official publication of IACIS—International Association of Computer Information Systems. Retrieved October 15, 2006, from http://www.iacis.org/iis/2003_iis/PDFfiles/PerezBerryHollman.pdf.

Schweitzer, D. (2005). Addressing the Human Security Vulnerability. *Computerworld*, 39(42), p. 40.

- Stanton, J., Stam, K., Mastrangelo, P., & Jolton, J. (2005). Analysis of End User Security Behaviors. *Computers & Security*, 24(2), pp. 124-133.
- Taneja, A. (2006). Determinants of adverse usage of information systems assets: A study of antecedents of IS exploit in organizations. Ph.D. dissertation, The University of Texas at Arlington, Texas. Retrieved April 9, 2007, from ProQuest Digital Dissertations database. (Publication No. AAT 3221195).
- Thomson, M., & von Solms, R. (1998). Information Security Awareness: Educating Your Users Effectively. *Information Management & Computer Security*, pp. 167-173.
- Thornburgh, T. (2005). *Social Engineering: The "Dark Art"*, InfoSecCD Conference '04, October 8, 2004, Kennesaw, GA. Copyright 2005 ACM.
- Wilson, M., & Hash, J. (2003). *Building an Information Technology Security Awareness and Training Program* (NIST SP 800-50). Retrieved January 5, 2007, from <http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf>
- Wilson, M. & Hash, J. *Information Technology Security Awareness, Training, Education, and Certification*. Retrieved August 18, 2006 from <http://www.itl.nist.gov/lab/bulletns/bltnoct03.htm>
- Wulgaert, T. (2005). *Security Awareness—Best Practices to Serve Your Enterprise*. Rolling Meadows: Information Systems Audit and Control Association.