2010

Ascertaining the Relationship between Security Awareness and the Security Behavior of Individuals

Gordon J. Grant
Nova Southeastern University, ggrant2118@aol.com

Ascertaining the Relationship between Security Awareness and the Security Behavior of Individuals

by

Gordon J. Grant

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

Graduate School of Computer and Information Sciences
Nova Southeastern University

2010

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

William L. Hafner, Ph.D. Chairperson of Dissertation Committee	Date
Maxine S. Cohen, Ph.D. Dissertation Committee Member	Date
Marlyn Kemper Littman, Ph.D. Dissertation Committee Member	Date

Approved:

Leonidas Irakliotis, Ph.D. Dean	Date

Graduate School of Computer and Information Sciences
Nova Southeastern University

2010

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

Ascertaining the Relationship between Security Awareness and the Security Behavior of Individuals

by
Gordon J. Grant

May 2010

Security threats caused by the inappropriate actions of the user continue to be a significant security problem within any organization. The purpose of this study was to continue the efforts of Katz by assessing the security behavior and practices of working professionals. Katz conducted a study that assessed whether the faculty and staff at Armstrong Atlantic State University had been performing the simple everyday practices and behavior necessary to avert insider threats to information security. Critical in understanding human behavior is in knowing how behavior varies across different groups or demographics. Because a user's behavior can be influenced by demographic groups, this study adapted Katz's study by examining the influence on the security behavior of four demographic groups identified by gender, age, education, and occupation. Like Katz, this study used a 5-point Likert scale quantitative self-administered, closed-ended questionnaire to assess the participants' security practices and behaviors. The questionnaire was developed in two sections: Section 1 used a binary scale to gather the participants' demographics data while Section 2 used a 5-point Likert scale to measure the participants' security behaviors. The sample population was derived from working professionals at the General Dynamic and Program Manager Advanced Amphibious Assault (GD & PM AAA) Facility in Woodbridge, Virginia. The total population at PM AAA Office was 288, of which 87 or 30% completed the survey. Results of the demographic survey indicate that (a) women were more security aware than their male counterparts, (b) younger participants were more security aware than their older counterparts, (c) participants who did not attend college were more security aware than their college-educated counterparts, and (d) participants in nontechnical positions were more security aware than their counterparts in technical positions. The results indicate that a relation exists between the participants' security behaviors and their levels of security awareness.

Acknowledgments

Completing this dissertation was a long and interesting journey that started in 1992, when the school was still called Nova University, classes where in trailers and 9600 baud rate was considered fast. This dissertation would not have been possible without the assistance, guidance, and support of many people.

Without the guidance and encouragement of my dissertation chair, Dr. William Hafner, and committee members, Dr. Marlyn Littman and Dr. Maxine Cohen, this dissertation would not have been possible; I am truly grateful to them.

I will always appreciate the support of my colleagues and friends—Lanny Gorr, Dan Moody, Dr. William Wright, William Sobotka, Lynn Robbins, and Charles Brown—who provided vital assistance throughout the study, especially those whom I used as a sounding board. Thank you.

Finally and most importantly, thank you to my Lord Jesus and my family who deserve special recognition. First, I want to thank Jesus without whom nothing is impossible. There was never any intention to go beyond a bachelor's degree, but I guess the Lord had other plans when He guided me to Nova Southeastern University. He instilled in me not only the desire but the fortitude, strength, and patience to complete this long and interesting journey. Thank you to my wife, for encouraging me to go back and finish this program, if she had known then that this dissertation would become a jealous mistress, she may not have been so encouraging. To my children for their patience and understanding, especially when Dad was busy reading research articles at their soccer games, thank you.

Again, I thank all of these persons for their support and encouragement.

Table of Contents

List of Tables

Tables

List of Figures

Figures

Chapter 1

Introduction

Statement of the Problem Investigated and Goal that Was Achieved

Security threats caused by a user's inappropriate action continue to be a significant security problem within any organization (Andrews & Whittaker, 2004; Blyth & Kovacich, 2006). These security threats are difficult to detect because they originate within a network or organization (Carroll, 2006). Inappropriate actions are defined as the actions performed by a user (e.g., downloading unauthorized software, reconfiguring a computer's security settings, disabling a firewall, providing personal information, or the disclosure of passwords) that can affect a system's security settings or generate a security breach (Blyth & Kovacich, 2006; Carroll, 2006). The intent of this study was to determine whether the individual user is using proper security behavior and practices necessary to avert inappropriate actions that lead to internal security threats. To better understand the inappropriate actions by a user (e.g., reconfiguring the security setting or disclosing a password), the author examined the relation between users' security behaviors and their awareness levels.

Defending against security threats resulting from the poor judgment or inappropriate actions of a user has traditionally been the responsibility of the network administrator and security personnel. In the 1990s, the interconnection of multiple networks (which until then were somewhat isolated) and the proliferation of cyber attacks shifted the security

community focus from system to network security (Arce, 2003). Besides dealing with a proliferation of cyber attacks, security personnel must also deal with extensive web browsing, instant messaging, peer-to-peer networks, digital media players, personal digital assistants (PDAs), wireless devices, and a host of software applications that interact directly and indirectly with internal networks and the Internet (Arce, 2003; Arce, 2004; Crossler & Belanger, 2006). In addition, the constant changes to newer technologies is also making it more difficult for even the most dedicated of security professionals to gain and maintain the knowledge and skills needed to allow them to carry out their security tasks effectively (Blyth & Kovacich, 2006). As a result, network administrators and security professionals continue to be in a state of constantly reacting to the latest technical changes and cyber attacks (Raghavan, Sakaguchi, & Mahaney, 2008). Consequently, responsibility for the security or information assurance of an information system has shifted from the organization's security personnel to the system user, who is perhaps the least trained or experienced in security matters within an organization (Andrews & Whittaker, 2004; Arce, 2003). This shift in responsibilities introduces a new set of security problems; specifically, the inappropriate actions of users, such as disabling a firewall, providing personal information, or the disclosure of passwords, are generating security breaches that can affect the entire organization.

To compound the security situation, users are also being targeted by hackers who are using social engineering attack techniques to influence the user to perform inappropriate actions that can generate security breaches. Bruce Schneier of Counterpane Internet Security stated that "amateurs hack systems, while professionals hack people" (Tucker, 2002, p. 10). Social engineering is the practice of using deception or persuasion to obtain

goods and information fraudulently (Twitchell, 2006). Some hackers also use a combination of social engineering with phishing schemes that use spoofed e-mails to lure users to fake websites designed to capture sensitive information or to load a virus that can create security breaches onto the workstation (Ohaya, 2006). These security breaches may allow unauthorized access from potentially anywhere in the world and corruption of data without physical access (Dark, Harter, Morales, & Garcia, 2008). Renowned hacker Kevin Mitnick indicated that, for him, resorting to a technical attack was rare because the use of social engineering was quicker and often more successful (Twitchell, 2006).

To mitigate the impact of social engineering attacks, private, academic, and federal organizations must set ground rules for user behavior through security training combined with security policies (Al-Hamdani, 2006; Mitnick & Simon, 2002; Ohaya, 2006). To mitigate the impact of inappropriate actions, all organizations must provide individuals with security training in the knowledge and skills needed to be able to recognize and know how to prevent inappropriate actions (Al-Hamdani, 2006; Mitnick & Simon, 2002; Ohaya, 2006). Today, private and federal organizations are using online information assurance electronic training (e-training) to increase the security awareness of their employees concerning the dangers of inappropriate actions (Ramim & Levy, 2006). This online security e-training is intended to provide individuals with the skills needed to recognize inappropriate actions and the knowledge of what they should do when confronted with security threats (Blyth & Kovacich, 2006).

Current articles on the security behavior and practices of the user have failed to consider how the user views security (Gross & Rosson, 2007a). Most information security research has focused on such technical issues as access to information systems

and secure communications (Siponen & Oinas-Kukkonen, 2007). Furthermore, research articles and conferences have focused largely on human memory, attitudes, and behaviors that are applicable to technical issues (Bishop & Frincke, 2005; Conti & Sobiesk, 2007; Kostakos & O'Neill, 2008). Research regarding user security behavior includes the following:

- Surveying professionals to analyze their perspectives on security management (Gross & Rosson, 2007a);
- Surveying users via an Internet survey provider to assess their ability to differentiate between privacy and security problems (Gross & Rosson, 2007b);
- Surveys of Information Technology (IT) students, faculty, and staff in an academic environment on their information security behaviors and practices (Katz, 2005; North, George, & North, 2006, 2007; Reeder & Arshad, 2005); and
- A study that focused on the behavior and practices of security personnel at various private organizations (Suchan, 2003).

Before security threats resulting from users' poor judgment or inappropriate actions can be resolved, a baseline of the individual user security behaviors and practices must be determined.

The goal for this study was to measure users' information security behavior and practices and to determine the information security awareness levels of users. Doing so was accomplished by using a quantitative survey instrument that measured users' security behaviors and practices according to demographic groups. The sample population for this survey was from the Program Manager Advanced Amphibious Assault (PM AAA) Office of the General Dynamics (GD & PM AAA) Facility in Woodbridge, Virginia.

The data collected were analyzed to determine the users' levels of information security awareness.

Relevance, Significance, or Need for the Study

Threats to information security are continuously growing and vary from organization to organization, but the one threat that remains the same, regardless of the type of organization, is the insider threat (Carroll, 2006), which, resulting from poor judgment or inappropriate actions by a user, continues to be a significant security problem within all types of organizations (Aytes & Connolly, 2004; Doherty & Fulford, 2005; Stoll, Tashman, Edwards, & Spafford, 2008). Security threats, such as downloading unauthorized software, reconfiguring security settings, or disclosing passwords, can make a system vulnerable to attack, resulting in data manipulation, modification, destruction, and theft (Doherty & Fulford, 2005). Such insider security threats are well documented (e.g., Arce, 2003; Mitnick & Simon, 2002; Ramim & Levy, 2006). However, additional research on approaches that potentially reduce or eliminate threats and intrusions remains necessary (Doherty & Fulford, 2005; Knapp, Marshall, Rainer, & Ford, 2007).

In 1998, Presidential Decision Directive 63 (PDD-63) established the nation's initial goal for information assurance and a cooperative framework between industry, academia, and local and national governments to protect the nation's critical infrastructure systems (Herrmann, 2002). Therefore, organizations are using information assurance to protect their critical infrastructure systems. Information assurance is a security technique that encompasses a defense-in-depth strategy composed of three components: technology, operations, and people (Andrews & Whittaker, 2004; Blyth & Kovacich, 2006). In the

past, the security community relied solely on technology to provide fast solutions to security breaches (John, Maurer, & Tessem, 2005; Siponen & Oinas-Kukkonen, 2007). However, people are part of the system, and failure to recognize this fact and address the training of users can result in disaster (Bishop & Frincke, 2005; Katz, 2005). Until the security community addresses the people component, comprehensive security strategies cannot be developed (Arce, 2003; Blyth & Kovacich, 2006). Thus, determining whether users are engaging in proper information security behavior and practices is necessary, and if they are not, appropriate recommendations to correct any flaws in their behaviors and practices should be made.

The significance of this study lies in its assessing user security behaviors and practices. The results of this study provide security personnel in the private, academic, and government community with an information-assurance baseline for security behaviors and practices of users. Results of this study also can provide organizations with snapshots of the current state of their employees' security behaviors and a basis for future research.

Barriers and Issues

One of the barriers to establishing sound user security behaviors and practices is the mindset of the security community and researchers (Hazari, 2005). User security behavior has received little attention from researchers because information security is considered a technical discipline, with much of the attention being focused on such topics as access control, password protection, data protection, and encryption (Hazari, 2005; Katz, 2005; Siponen & Oinas-Kukkonen, 2007). Another barrier is the mindset of senior

managers who fail to see information security as a "value added" contribution to the organization's "bottom line" (Jahankhani, Fernando, Nkhoma, & Mouratidis, 2007). In fact, computer crimes often go unreported because managers and organizations are not willing to risk public embarrassment or bad publicity (Hazari, 2005; Kshetri, 2006).

Earlier studies on such demographics as age and gender in terms of how they impacted computer usage may no longer be accurate (Knight & Pearson, 2005). Knight and Pearson stated that changing demographics in the workplace and their effect on the organizations (e.g., the increase in the number of women and age) should be reexamined. In addition, the constant upgrades to newer technologies and changes in security (e.g., upgrades, patches, and applications) make information security an ever-changing and fast-moving environment (Al-Hamdani, 2006; Blyth & Kovacich, 2006). These ongoing technology upgrades may frustrate users and security personnel who have to keep up with all the changes. This fluid security environment may cause the user to become either apathetic or hostile towards security (Gross & Rosson, 2007a; West, 2008).

One issue for this study is the reluctance or lack of responsiveness of individuals to participate in surveys and studies (Creswell, 2003; Locke, Spirduso, & Silverman, 2000; Nardi, 2003). This reluctance to participate arises from participants' tending to (a) distrust surveys, especially when the surveys address topics the participants are not as knowledgeable in as they should be; (b) be uneasy in acknowledging and sharing bad practices; and (c) be apprehensive as to who will see the results of the survey (Reeder & Arshad, 2005; Shneiderman & Plaisant, 2005).

Research Question Investigated

The purpose of this study was to use a quantitative, closed-ended, survey instrument to measure users' security behavior according to different demographics. The users' behavior data were then analyzed to determine users' levels of security awareness. Measuring behavior is normally accomplished through the use of a questionnaire (Nardi, 2003; Singh, Cabraal, Demosthenous, Astbrink, & Furlong, 2007). The variables for this study include an independent variable—the security behavior of a user—and a dependent variable—the security awareness level of a user. The demographics for this study include age, gender, education, and occupation and provide a framework to answer the following questions:

- Are female users more security aware?
- Are users age 40 and over more security aware?
- Are users with higher levels of education more security aware?
- Are users in technical positions more security aware?

The intent of this study was to answer the following research question:

- Is there a relation between users' security behaviors and their levels of security awareness?

Limitations and Delimitations of the Study

A limitation (restriction) that may affect this study but is beyond the control of the researcher was the participants' responses to the survey. Past research has indicated that even trained security personnel are resistant in providing any information regarding their

information security behaviors and practices (Katz, 2005). The delimitations for this study, those elements within the control of the researcher, include the following:

- The study was conducted with one sample population in Virginia.
- Participants' access to the survey was via a secure intranet.

Definition of Terms

Key terms used throughout this dissertation are identified and defined below.

Cyber attack – This term denotes illegal activities or a crime that takes place on an information system, such as theft of software, data, unauthorized access, or modification of information (Blyth & Kovacich, 2006).

Hacker – A *hacker* is a person who uses and creates computer software for enjoyment or to gain access to information illegally (Whitman & Mattord, 2003).

Hacking – Hacking is the act of gaining access to a computer illegally (Whitman & Mattord, 2003).

Identity theft – Identity theft is a crime in which one person masquerades under the identity of another (Campbell, Calvert & Boswell, 2003).

Information assurance (IA) – Information assurance is an information security technique that protects and defends information and automated systems by ensuring their confidentiality, integrity, availability, authentication, and nonrepudiation and includes the restoration of information and systems by incorporating protection, detection, and reaction capabilities (Herrmann, 2002).

Information security – Information security refers to protection of information systems against unauthorized access, transfer, destruction, or modification of

information, whether accidental or intentional, in a storage, processing, or transit state (Blyth & Kovacich, 2006).

Infrastructure system – This term refers to a network of independent, largely privately owned, automated systems and processes that function collaboratively and synergistically to produce and distribute a continuous flow of essential goods and services (Hermann, 2002).

Internet – The *Internet* is a complex, diverse, wide area network (WAN) that connects local area networks (LANs) and individual users around the globe (Dean, 2003).

Phishing – Phishing is a cyber attack that mimics a legitimate or trusted website to convince victims to disclose their user ids, passwords, or personal information; it is also being used in conjunction with social engineering attacks (Levy, 2004; McDowell, 2006).

Security awareness – Security awareness occurs when a user understands the security policies, procedures, and practices in order to make sound judgments when a potential security issue occurs in the absence of guidance (Boyce & Jennings, 2002).

Security education training and awareness - This process instructs users in their responsibility to uphold the organization's information system and security policies, procedures, and practices (Boyce & Jennings, 2002).

Social engineering – Social engineering refers to an attack technique used to target the individual, with the aim of stealing personal or corporate information; its action can be as simple as asking the victim for information or can be combined with a phishing cyber attack (e.g., an e-mail that promises new application features under a free trial basis) in order to steal the user's name, password, or other personal information (Mitnick & Simon, 2002).

Spyware – *Spyware* is an ad-based program that arrives through e-mail, enticing the user to install or link to free software. Spyware can also arrive via instant messaging, popular downloads, online gaming, and porn sites. Spyware is designed to track what the user does, where the user goes, and what information the user transmits, which is sent back to the hacker (McDowell, 2006).

Threat – A *threat* is the potential danger that a vulnerability may be exploited intentionally, triggered accidentally, or otherwise activated (Herrmann, 2002).

User – This term refers to any individual or employee who uses an information system (computer) locally or across the Internet for business or personal use (Blyth & Kovacich, 2006; Boyce & Jennings, 2002).

Vulnerability – A *vulnerability* is a weakness in a system that can be exploited to violate the system's intended behavior relative to safety, security, reliability, availability and integrity or to obtain access to some asset (Andrews & Whittaker, 2004).

Summary

Today's network administrators and security personnel are being overworked. In addition to their day-to-day operations, they must also deal with rising Internet usage, escalating software upgrades, rapid introduction of new technologies, and increasing numbers of cyber attacks (Arce, 2003; Arce, 2004; Crossler & Belanger, 2006; Raghavan et al., 2008). Consequently, responsibility for a system's information assurance has shifted to the user, who is considered the least trained or experienced in security matters (Andrews & Whittaker, 2004; Arce, 2003). This shift of responsibility is introducing a new set of security problems, specifically, the inappropriate actions of the user. Security

threats due to the poor judgment or inappropriate actions of users (e.g., reconfiguring security settings or disclosing passwords) continue to be a significant security problem within any organization (Aytes & Connolly, 2004; Doherty & Fulford, 2005; Stoll et al., 2008). These security threats have the potential to cause great loss to the organization and the user in the forms of data manipulation, modification, destruction, or theft (Doherty & Fulford, 2005). Because these security threats are well documented (e.g., Doherty & Fulford, 2005; Knapp et al., 2007), there is a pressing need for more research that can highlight strategies or approaches that might reduce these threats.

However, existing work on user security practice has failed to consider how users view security (Gross & Rosson, 2007a). Most information security research has focused on such technical issues as access to information systems and secure communications (Siponen & Oinas-Kukkonen, 2007), but many nontechnical articles present themes that are directly applicable to technical issues (Bishop & Frincke, 2005). As Kostakos and O'Neill (2008) indicated, traditional human computer interaction (HCI) literature has considered human-in-the-loop security issues as a design problem in need of appropriate interfaces, interactions, and policies. Furthermore, Bishop and Frincke (2005) stated that, without understanding something about how people interact with security, it is easy to blame users for security breaches. Therefore, it is necessary to determine whether users are engaging in proper information security behaviors and practices and, if not, to make appropriate recommendations to correct any flaws in their behaviors and practices. Before these inappropriate actions can be resolved, an initial baseline of the common user security behaviors and practices must be determined. The goal of this study was to continue the efforts by Katz (2005) in assessing user information-security behaviors and

practices in order to determine the information-security awareness level of users in an organization, specifically according to demographic group.

Chapter 2

Review of the Literature

This chapter presents a summary of the published research in the area of information security and, specifically, on the behaviors and practices of individual users. After a section addressing the background information, the main topics include insider security threats, user behavior, and security awareness and training. The chapter concludes with a summary of what is known and unknown in research literature, the contribution of this study, and a chapter summary.

Background

Threats can be classified into three broad categories: natural, internal, and external (Blyth & Kovacich, 2006). The natural threat is, as the name implies, any natural disaster—such as fire, flood, power failure, earthquake, and mudslide—that can cause damage or loss of data to a system. The internal or insider threat occurs when a party or person knowingly or unknowingly causes damage or loss of data to a system (Blyth & Kovacich, 2006). The external threat is the more familiar threat and includes a hacker trying to gain access to a system (Blyth & Kovacich, 2006; Carroll, 2006). Defending against these security threats has traditionally been the responsibility of the network administrator and the security personnel. Today, these network administrators and security professionals are being overworked (Raghavan et al., 2008). Besides having to

maintain their current network's security, personnel must also deal with extensive web browsing, instant messaging, peer-to-peer networks, digital media players, personal digital assistants (PDAs), wireless devices, a host of software applications that interact directly and indirectly with internal networks and the Internet, unknown software flaws that can create security threats, and a proliferation of cyber attacks (Arce, 2003).

In addition to this increased workload, the continuing escalation of newer technologies and security tools is also making it more difficult for even the most dedicated of security professionals to gain and maintain the knowledge and skills needed to allow them to effectively carry out their security tasks (Al-Hamdani, 2006; Blyth & Kovacich, 2006). Because security risks can change as quickly as new threats, vulnerabilities, and attack tools are introduced, security must now be designed as a continuous process that reacts quickly to changes (Al-Hamdani, 2006; Raghavan et al., 2008). All these security issues, in conjunction with an existing acute shortage of administrators and security personnel, are compelling organizations to shift the responsibility of information system security to the user, who is perhaps the least trained or experienced in security matters (Arce, 2003). This shift in responsibilities is exposing the organization to the possibility of increased insider security threats and, specifically, to the inappropriate actions of users (Andrews & Whittaker, 2004; Blyth & Kovacich, 2006).

Insider Security Threats

Threats to information security are always increasing and vary from organization to organization, but the one threat that remains the same regardless of the type of

organization is the insider threat (Carroll, 2006). Insider security threats may not occur as frequently as external attacks, but they have a higher rate of success, can go undetected and pose a greater risk than an external attack (Chinchani, Iyer, Ngo, & Upadhyaya, 2005). Insider threats can be classified into two categories: the intentional and the unintentional threat (Carroll, 2006). The intentional threat occurs when a party or trusted person within the organization knowingly sets out to cause damage or loss of data to a system (Blyth & Kovacich, 2006). The intentional threat can be anything from an employee creating a security risk for malicious reasons or personal gain to the more familiar threat of a hacker trying to gain access to a system (Blyth & Kovacich, 2006; Carroll, 2006). The intentional threat is a more serious threat to information security in that hackers and criminals have learned to manipulate users into divulging confidential information with a technique called social engineering (Aytes & Connolly, 2004). As Bruce Schneier of Counterpane Internet Security stated, "[A]mateurs hack systems, while professionals hack people" (Tucker, 2002, p. 10). Renowned hacker Kevin Mitnick indicated that, for him, resorting to a technical attack was rare because the use of social engineering was quicker and often more successful (Twitchell, 2006).

Trust plays a key role in the user's decision-making process (Tsai & Egelman, 2006). Trustworthy users can fail to be trustworthy when it comes to protecting their systems due to inadequate education, negligence, and various social pressures (Orgill, Romney, Bailey, & Orgill, 2004). Furthermore, the trust that people put in websites has enabled hackers to easily deceive people at all levels of income and education (MacInnes, Musgrave, & Laska, 2005). Social engineering attacks exploit the user's trust by influencing the user to perform inappropriate actions so that information can be stolen or

security breaches can be generated (Orgill et al., 2004; Twitchell, 2006). Some hackers also use a combination of social engineering with phishing attacks that use spoofed e-mails to lure users to fake websites designed to capture sensitive information or to load a virus onto the workstation, thereby creating security breaches (Kumaraguru et al., 2007; Ohaya, 2006). These security breaches may allow unauthorized access from potentially anywhere in the world and corruption of data without physical access (Dark et al., 2008). Studies have indicated that a large number of people fall for these phishing attacks even when the participants are made aware that their ability to identify phishing attacks is being tested (Kumaraguru et al., 2007). Many of these phishing attacks were not even detected; therefore, things may be worse than reported because attackers are often able to hide their tracks by disabling logging facilities or modifying event logs so their activity goes undetected (Kemmerer, 2003). To mitigate the impact from social engineering attacks, organizations must set ground rules for user behaviors through the use of security training combined with security policies (Al-Hamdani, 2006; Mitnick & Simon, 2002; Ohaya, 2006).

The unintentional threat occurs when a trusted person within the organization causes damage or loss of data or service without direct intent (Blyth & Kovacich, 2006). Unintentional threats can be caused by anything from leaving a laptop or sensitive document unattended, to inadvertently installing software with an unknown flaw or bug that can create a security risk (Andrews & Whittaker, 2004; Blyth & Kovacich, 2006). Other unintentional threats from due to users' poor judgment include opening e-mail attachments without checking for viruses, downloading unauthorized software, reconfiguring the system security setting, disabling a firewall to access an unauthorized

website, and providing personal information or a password to a coworker (Blyth & Kovacich, 2006; Carroll, 2006). As more users become responsible for their own system security, the number of unintentional security threats will increase (Chinchani et al., 2005). Because organizations have their information infrastructure connected, the unintentional threat by one user can lead to a security breach affecting the entire infrastructure (Aytes & Connolly, 2004). These security breaches have the potential to generate great loss for the organization and the user in the form of data manipulation, modification, destruction, or theft (Chinchani et al., 2005; Doherty & Fulford, 2005; Gross & Rosson, 2007a). Carroll (2006) stated that the unintentional compromise of information by an insider can be a product of a lack of security awareness or a failure to adhere to security policies. To overcome these unintentional threats, the security community must understand the mindset or behavior of the user in order to develop appropriate security countermeasures (Conti & Sobiesk, 2007; Vatsa, Sural, & Majumdar, 2007). These insider threats are creating a pressing need for more research that can highlight strategies or approaches that might reduce the insider threat (Doherty & Fulford, 2005; Knapp et al., 2007).

In 1998, Presidential Decision Directive 63 (PDD-63) established the nation's initial goal for information assurance and a cooperative framework for industry, academia, and local and national governments to protect the nation's critical infrastructure systems (Herrmann, 2002). Therefore, organizations are using information assurance to protect their critical infrastructure systems. Information assurance is an information security technique that encompasses a defense-in-depth strategy composed of three components: technology, operations, and people (Andrews & Whittaker, 2004; Blyth & Kovacich,

2006). These components form the foundation and framework for developing a comprehensive security strategy (Blyth & Kovacich, 2006).

In the past, the majority of security threats were external and could be prevented or solved by using technical solutions such as firewalls and antivirus software (Arce, 2003). Current technical solutions are using mathematical approaches that include biometrical authentication, virtual private networks, and cryptographic techniques (Siponen & Oinas-Kukkonen, 2007). Detecting the insider threat, however, is more difficult because there is no way to monitor a person's actions or intent (Carroll, 2006). Most attempts in preventing insider threats involve (a) technical solutions such as firewall logs, intrusion detection systems (IDS), and honeypots or (b) security policies such as procedures that govern the actions and behavior of personnel within an organization (Carroll, 2006; Doherty & Fulford, 2005; Stahl, 2004). Technical solution such as honeypots can be designed to detect, identify, and confirm insider threats (Spitzner, 2003). Restraints on these technical solutions include the insider threat bypassing or introducing bogus or false information to mislead security personnel (Spitzner, 2003). On the other hand, restraints in implementing security policies include (a) cost—implementing policies takes time and money that are usually unbudgeted—, (b) organizational priorities—ongoing projects cannot be interrupted for the sake of imposing standards—, (c) policy age—policies should be updated regularly to reflect current technologies and security situation—, and (d) enforcement—policies by themselves are not very useful if not enforced (Carroll, 2006; Doherty & Fulford, 2005; Moore, 2004; Stefanek, 2002). Understanding users' behavior in security decision making is an avenue that may improve training in user-security behavior (West, 2008).

User Behavior

Insecure behavior by individual users is now considered one of the major chinks in the armor of computer-security countermeasures (Aytes & Connolly, 2004). Carroll (2006) indicated that personnel are among the biggest threats to the information security of an organization. In addition, Bishop and Frincke (2005) stated that, ultimately, information security is more about people than computers and information. Thus, security solutions that fail to take human nature into account are doomed (Bishop & Frincke, 2005). However, very little is known about why users choose to engage in unsafe security behavior (Aytes & Connolly, 2004). Two reasons for why proper security behavior is difficult to achieve include the mindset of the user and management. User mindset includes (a) user attitude—that is, inappropriate actions continue because many users, despite having little to no formal training in computer security, feel relatively comfortable in their ability to protect themselves from viruses, computer crashes, and password violations (West, 2008)—, (b) security risk—that is, many users believe that they are not at risk because they generally do not understand security risk: The components of security risk such as threats, vulnerabilities, and the value of information are poorly understood and are often misjudged (West, 2008)—, (c) lack of motivation—most users are either intimidated by the very concept of networking or they simply do not care enough about the topic to actively learn (West, 2008)—, (d) user priorities—users are usually busy with their assignments with little time for security training, so they resist such training (Tucker, 2002)—, and (e) user indifference—that is, users who simply refuse to comply with an organization's information security policies and procedures can

frustrate the security manager who spent the time in creating these policies and procedures (Tucker, 2002).

Management mindset includes management resources, cost of security, and security priorities. In terms of management resources, despite increased security threats, organizations traditionally allocate very little of the IT budget to information security. In fact, the average amount of money as a percentage of revenue spent on security is 0.0025%, or slightly less than what is spent on coffee (Hazari, 2005). Furthermore, because security costs time and money, business managers often forgo security in order to implement a system or service that is faster and cheaper (Stefanek, 2002). In terms of security priorities and support, network administrators often have limited resources, making user security training the first casualty as departments trim projects (Tucker, 2002). In addition, shrinking IT budgets are forcing IT directors to reduce staff by eliminating the more expensive qualified employees and replacing them with less expensive untrained or unqualified employees, at the risk of leaving security training to unqualified or untrained personnel (Stefanek, 2002). Moreover, IT managers often struggle with getting fellow department managers to provide time for employees to receive security training (Stefanek, 2002). Finally, IT managers have come to depend on technology to solve their security problems. However, they might have difficulty justifying new security equipment, such as firewalls or intrusion detection devices, if user security training increases security (Paulson, 2002).

Because people are part of the system, failure to recognize and address the security aspects of the end user can result in disaster (Bishop & Frincke, 2005; Katz, 2005). Security risks associated with human behavior include the following:

- Social engineering—a hacking technique that exploits human trust or ignorance in order to obtain information or gain access to information (Dean, 2003; Tucker, 2002).
- Misuse of system and network—users consuming valuable computer resources such as Internet connectivity or storage space for illegal purposes such as sharing MP3 files or games. In addition to consuming costly resources, this behavior potentially exposes systems to security threats and violates laws (Tucker, 2002).
- Password guessing—users often choose passwords that are easy to guess or crack (Dean, 2003; Tucker, 2002).
- Physical access to bypass controls—users often leave documents and laptops unsecured or set up their systems in insecure areas (Dean, 2003; Tucker, 2002).
- System configuration—users often operate their computers with out-of-date antivirus software, fail to install security patches, or open files without checking for viruses, worms, and Trojan horses. These problems pose perhaps the greatest security threat to a system (Reeder & Arshad, 2005).

Although organizations are providing security training for their users, these same users continue to disable security settings in order to access unauthorized websites and download unauthorized web applications, such as music and video files, behaviors that increase the risk of security breaches (Balfanz, Durfee, Smetters, & Grinter, 2004; Cranor & Garfinkel, 2004). Smith (2003) stated that younger users who had grown up with computers perceived security as an obstacle they had to work around. For them, information security is often considered inconvenient, not only for the end users, but also for the system administrators and application developers as well (West, 2008). Most

users will often sacrifice security and privacy for convenience while most network managers will willingly sacrifice speed for security or vice versa, depending on the priority of the user or organization (Jungck & Shim, 2004; Van Dyke, 2007). Other factors that influence user behavior towards security include perceptions, understanding, and trust (Gross & Rosson, 2007a). Cyber attacks such as social engineering can also influence user actions (West, 2008).

How people perceive security risks guides their actions, with most users believing that they and their organizations are safe from security threats (Havana & Roning, 2004; West, 2008) because a good security program is transparent. Unless the system crashes, there are no indicators that the system is secure (Paulson, 2002; West, 2008). Furthermore, if there are no visible threats, most users believe they are not at risk (West, 2008). These assumptions create a mindset with both managers and users who believe that, if a cyber attack has not yet happened, it is unlikely to happen in the future (Stefanek, 2002).

Although users claim that security and privacy are important to them when online, these same users seem to be at ease in disclosing personal information in order to gain additional products or services when registering for online accounts (Conti & Sobiesk, 2007). These users believe that they are less vulnerable to security risks because they have nothing of interest on their system that anyone would want to steal (Havana & Roning, 2004; West, 2008). These inconsistencies between professing privacy concerns and engaging in risky behavior while on the Internet may be more a consequence of ignorance rather than irrationality (Van Dyke, 2007). Research has indicated that, despite having little to no formal training in computer security, most users feel relatively

comfortable in their ability to protect themselves from viruses, computer crashes, and password violations (Aytes & Connolly, 2004; West, 2008). Users have also been known to perform low-level, insecure behavior such as password sharing, creating and using weak passwords that can be easily guessed, opening e-mail attachments without checking for viruses, and so forth without any attacks on their systems (Aytes & Connolly, 2004). Because these actions are not discouraged and, in some cases, are rewarded because they are seen as helpful (in cases of sharing passwords) or as saving time by not scanning for viruses, they can further encourage inappropriate actions or justify the negative attitude towards security (Aytes & Connolly, 2004).

In an organizational setting, user behavior is also influenced by different levels of culture, ranging from professional and organizational levels to the group level. That is, for a specific project, the culture of the project team will dominate the behavior and practices of the individual (Karahanna, Evaristo & Srite, 2005). Other impacts to security behavior include users' limited capacity for information processing and routinely performing multiple tasks at once (West, 2008). As a result, few tasks or decisions receive full attention at any given time, and people tend to favor quick decisions based on learned rules and heuristics (West, 2008). Because of this tendency, users often fail to recognize security risks because they do not understand the technology or the risks so basically believe that they are at less risk than others (Van Dyke, 2007; West, 2008). The average user also faces a dilemma when making security decisions. That is, users generally lack both the motivation and technical knowledge to make informed decisions on their own (Ohaya, 2006; Stoll et al., 2008; West, 2008) because they do not have the underlying knowledge of how operating systems, e-mail, and websites work (Ohaya,

2006). In addition, the mechanisms for encryption, authentication, and authorization can be difficult for the user to understand and use (West, 2008). Setting up security is still much too complicated for the common user (Lampson, 2004).

Furthermore, studies have indicated that the more complex the security mechanism, the less it is used (West, 2008). For this reason, nonacceptance of security tools is recognized as a major problem facing the security community (West, 2008). As a result, improper perceptions about security and poor or even moderate attitudes towards security often lead to very poor protection (West, 2008). The most elegant and intuitively designed interface does not improve security if users ignore warnings, choose poor settings, or unintentionally subvert corporate policies (West, 2008). Simply being aware of security threats and vulnerabilities and having the knowledge and ability to mitigate these security risks does not guarantee any action will be taken by the user (West, 2008). Because people's morals and ethics vary from person to person, relying on the employee to do what is right or ethical is never the answer (Carroll, 2006). To ensure that an employee will make the right decision when confronted with a security threat, that employee needs to participate in a security education program (Boyce & Jennings, 2002).

Security Awareness and Training

To counter the security risks posed by inappropriate user action, security professionals propose security awareness and training programs for users (Aytes & Connolly, 2004; Blyth & Kovacich, 2006; North et al., 2007). Awareness programs consist of newsletters, posters, flyers, and lectures while training programs are more involved and may include case studies and hands-on training (Crossler & Belanger,

2006). The primary goal of security-training programs is to make the user aware of the various security risks and how they could affect the organization (Aytes & Connolly, 2004). Prior to conducting any security training, an organization security manager must assess the organization's state of security awareness (Blyth & Kovacich, 2006). Tucker (2002) reported that a simple method for assessing security awareness is for the security manager to consider whether a typical employee observing another employee doing something that might be inappropriate be able to answer the following three questions:

- Would this employee know whether the activity was wrong?
- Would this employee choose to report the misuse of the system?
- Would this employee know how to report the incident?

These questions strike at the heart of security awareness. Users must understand and recognize not only unacceptable behavior but also common threats and vulnerabilities (Blyth & Kovacich, 2006; Conti & Sobiesk, 2007; Tucker, 2002). Users must know when not to execute a dangerous e-mail attachment or install a software patch, and they must know how to take appropriate action when confronted with a threat (Aytes & Connolly, 2004).

A good information security-awareness program is more than simply ensuring that everyone knows and obeys the security rules (e.g., rules for user behavior, policies, and procedures), it involves providing the reason behind the security rules in order for users to make sound security decisions in the absence of specific guidance (Boyce & Jennings, 2002). Raising the user level of security awareness will provide that user with the knowledge to be able to recognize and prevent inappropriate actions (Al-Hamdani, 2006). Security awareness should help curtail inappropriate user behavior, prevent the user from

creating system security vulnerabilities, and protect the user from becoming the next victim of a cyber attack (Blyth & Kovacich, 2006; Hazari, 2005).

Besides developing information security awareness programs, organizations must continually assess the education and training needs of their users and security personnel (Dhillion & Hentea, 2005). Continuing education and refresher training is very important in keeping security personnel and users up-to-date on new applications, current security threats, regulations, and policies (Dhillion & Hentea, 2005; Lipinski, Cooper, Cook, & Orndorff, 2007). The biggest hindrance in implementing any security awareness and training program is in obtaining the participants' acceptance (Bradley & Lee, 2007). Even if security training is perceived as useful, it will only be accepted if it is also perceived as easy to learn and use (Bradley & Lee, 2007). Unfortunately, these security efforts and training programs are designed largely in the absence of reliable knowledge about the users' behavior that this training is seeking to enhance or change (Aytes & Connolly, 2004). Therefore, before these security awareness and training programs can be implemented, organizations need to assess the security behavior of individual users. In addition, to overcome the inappropriate actions of users, organizations need to embrace change related to their current security strategies even though organizations and users are renowned for their resistance to change (Ramim & Levy, 2006).

Summary of What Is Known and Unknown in Research Literature

Current literature on user security has received little attention from security researchers because information security is still considered a technical discipline (Siponen & Oinas-Kukkonen, 2007). Kostakos and O'Neill (2008) stated that traditional

HCI literature has considered the human-in-the-loop security issues as a design problem in need of appropriate interfaces, interactions, and policies. However, Bishop and Frincke (2005) stated that, without understanding something about how people interact with security, it is easy to blame users for security breaches. Articles on user behaviors regarding system security have indicated that individuals are still engaging in inappropriate security behavior. These inappropriate actions include the following: security personnel who are security certified tend to violate security procedures 50% more than their noncertified counterparts (Suchan, 2003); college students majoring in technical curriculums admitted to violating security procedures more than students not majoring in technical curriculums (North et al., 2006, 2007); and the faculty and staff at Armstrong Atlantic State University performed only minimum security practices to safeguard their information, including not using antivirus software, not backing up data, not using strong passwords, and not locking their systems when they were left alone (Katz, 2005).

Research on inappropriate user action regarding online protection, especially protection against phishing attacks, includes the following. Reeder and Arshad (2005) reported that 75% of the participants still fell victim to a mimicked phishing attack even though the researchers provided clues that it was an email scam. In addition, Kumaraguru et al. (2007) reported that participants still fell victim to a phishing attack even though they had received training and warnings about such attacks. Engelman, Cranor, and Hong (2008) reported that users heeded security warnings; however, if the user did not understand what a phishing attack was, that user would not pay attention to the security warning. Further, Wu, Miller, and Garfinkel (2006) reported that security

toolbars failed to prevent users from being spoofed by phishing attacks because users failed to respond to security toolbars. Finally, Dhamija, Tygar, and Hearst (2006) reported that standard security indicators were not effective for most users.

Furthermore, research has also been conducted on inappropriate user action regarding system authentication. Sasamoto, Christin, and Hayashi (2008) reported that users failed to conceal their actions when authenticating, increasing the risk in becoming a victim to shoulder surfing, and Moncur and Leplatre (2007) reported that some participants admitted to writing down their passwords or sharing their passwords. Toomim, Zhang, Fogarty, and Landay (2008) investigated shared access control using photo sharing and reported that vulnerabilities in guessing the shared password occurred. Finally, Jakobsson, Stolterman, Wetzel, and Yang (2008) proposed a preference-based authentication approach with an interactive session to help users remember their passwords; however, during testing, an adaptive robot was successful in guessing the answers to the questions.

In investigating the Threat, Awareness, Learning, and Control (TALC) system, which draws graffiti on the computer background wallpaper to denote potential vulnerabilities, Sankarapandian, Little, and Edwards (2008) reported that four out of seven users felt that using TALC had improved their ability to protect their computer. Furthermore, Stoll et al. (2008) reported, concerning a security decision tool called Sesame report, that it helped users make better security decisions. In addition, Herzog and Shahmehri (2007) investigated existing user help applications, techniques, and built-in security and reported that these applications may still be failures because actual implementation often disregarded usability guidelines. Finally, Gaw, Felten, and Fernandez-Kelly (2006)

report that participants felt paranoid when using an encrypted e-mail system and indicated that using encrypted e-mail messages was annoying and less efficient than sending plain old text e-mails messages.

Contribution of this Study

The goal of this study was to assess users' security behaviors in relation to their security awareness. The results of this study provide researchers and security personnel in the private, academic, and federal community with the following:

- A survey instrument to assess the everyday security behaviors and practices of working professionals;
- A demographic baseline on the security behaviors and practices of working professionals by gender, age, education, and occupation;
- An extension to the security behaviors and practices baseline developed by Katz (2005), from which further research can be conducted.

Summary

The decentralization of computers along with rising Internet usage, escalating software upgrades, rapid introduction of new technologies, and an increasing number of cyber attacks has overwhelmed security personnel (Arce, 2003; Raghavan et al., 2008). Because of these attacks, users are now responsible for their systems security or information assurance. This shift of responsibility is introducing a new set of security problems, specifically, the internal security threat caused by the inappropriate actions of users. Insider threats may not occur as frequently as external attacks, but they have a

higher rate of success, can go undetected, and pose a greater risk than external attacks (Chinchani et al., 2005). Insider threats can be classified into two categories: the intentional and the unintentional (Carroll, 2006). The intentional security threat occurs when a party or trusted person within the organization knowingly sets out to cause damage or loss of data to a system (Blyth & Kovacich, 2006). The unintentional security threat occurs when a trusted person within the organization causes damage, loss of data, or loss of service without direct intent (Blyth & Kovacich, 2006). These internal threats continue to be a significant security challenge within any organization.

Another challenge facing the security community is the gap of security knowledge that exists between security personnel and hackers. Because of this knowledge gap, hackers are creating cyber attacks faster than security personnel can react to them. In addition to these internal security challenges, hackers have shifted the focus of their attacks to users. Besides the user, organizations also seem to be unprepared to deal with such cyber attacks. One way to lessen the impact of these security challenges is through information assurance training. Information security training not only raises users' awareness level, but also provides users with the ability to recognize and prevent any inappropriate actions. However, prior to conducting any security training, an organization security manager must assess the organizations state of security awareness (Blyth & Kovacich, 2006).

Current literature on user security has received little attention from security researchers because information security is still considered a technical discipline (Siponen & Oinas-Kukkonen, 2007). For example, Kostakos and O'Neill (2008) stated that traditional HCI literature has considered the human-in-the-loop security issues as a

design problem in need of appropriate interfaces, interactions, and policies. However, Bishop and Frincke (2005) stated that, without understanding how people interact with security, it is easy to blame users for security breaches. Finally, articles on users' behaviors regarding system security have indicated that individuals are still performing inappropriate security behavior.

Chapter 3

Methodology

This chapter presents the methodology used for this research study. The goal of this study was to assess the security behaviors and practices of the working professional. Research can use a quantitative or a qualitative approach (Nardi, 2003; Creswell, 2003). The quantitative approach employs strategies of inquiry, such as experiments and surveys that collect data on predetermined instruments that yield statistical data (Creswell, 2003). The qualitative approach employs strategies of inquiry, such as narratives, phenomenology, or case studies that collect open-ended, emerging data with the primary intent of developing themes from the data (Creswell, 2003). Nardi (2003) stated that the use of a quantitative research instrument is the best approach for research intended to describe human behavior. The more efficient quantitative method for measuring attitude and behavior is to use a closed-ended questionnaire (Nardi, 2003). Although the closed-ended questionnaire allows for fewer variations in participants' responses, it is easier and quicker for the participants to complete (Nardi, 2003). Self-administered questionnaires are best designed for studying behavior that may be difficult for people to tell someone else about face-to-face (Nardi, 2003). In addition, the anonymity of self-administered questionnaires permits participants to be more candid, but researchers do not always know whether the participants are answering the questions honestly (Nardi, 2003).

Research Method Employed

The main purpose of this study was to assess the security behaviors and practices of the common system user. Previous research in assessing the security behavior of a user was conducted by Katz (2005). To measure the participants' security behavior, Katz used a 5-point Likert scale self-administered, closed-ended quantitative questionnaire. Because this study was a continuation of the work conducted by Katz, permission was obtained from Katz to adapt his methodology (see Appendix B). This adaptation was vital to maintaining the integrity of the baseline developed and helped establish a viable launching point for this study. The adaptation included replacing the physical security questions with questions regarding security training. Because users' behaviors can be influenced by their demographic groups, the adaptation also included examining the influence on the security behavior of four demographic variables: gender, age, education, and occupation. Like Katz, this study used a 5-point Likert scale in a self-administered, closed-ended questionnaire. The survey instrument was designed in two sections: The demographic section used a binary scale to gather the participants' demographic data, and the security section used the 5-point Likert scale to measure the participants' security behaviors. Details of the study's methodology are provided in the following sections.

Participants

The participants for this study were working professionals from the General Dynamic and Program Manager Advanced Amphibious Assault (GD & PM AAA) Facility in Woodbridge, Virginia. PM AAA is no different from any other organization that is responsible for securing information ranging from organizationally sensitive information

to personnel evaluations. The participants from PM AAA Office were selected because PM AAA is not only a research and development facility but also a paperless environment. Because the employees use computers on a daily basis, their computer skills and security knowledge should be good. The total population at the PM AAA Office was 288.

Privacy Protection

Research involving human subjects needs to have a research plan reviewed by the Institutional Review Board (IRB) of the researcher's institution and the participating organization's IRB or designated authority (Creswell, 2003). These IRB committees exist because of federal regulations that provide for the protection of human rights against violations (Creswell, 2003). To resolve any ethical issues concerning human rights violations and to protect the participants' privacy and anonymity, the survey was submitted to the PM AAA Operations Officer, who reviewed the survey and submitted it to the Program Manager (PM) for approval (see Appendix C). After PM AAA approval was received, the survey instrument was submitted to Nova Southeastern University (NSU) IRB for approval (see Appendix D). Upon notification of NSU IRB approval, the researcher conducted the survey.

Variables

Measuring behavior is normally accomplished through the use of a questionnaire that measures the variables among the demographics (Nardi, 2003; Singh et al., 2007). The variables for this study include an independent variable—the security behavior of a

user—and a dependent variable—the security awareness level of a user. The independent variable or security behavior by demographics was collected from the survey questionnaire. The dependent variable or security awareness level was determined from the tabulated results of the survey instrument.

Survey Instrument

The survey instrument was an adaptation of the questionnaire developed by Katz (2005). To increase the response rate, the researcher limited the questions in each section to one page (Kruck & Teer, 2008). The survey instrument consisted of (a) a cover sheet, (b) a demographic section, and (c) a security section (see Appendix E).

Cover Sheet

The cover sheet included (a) a statement informing the participant that the survey was for a doctoral dissertation, (b) a statement that all information collected would be confidential, (c) a participation consent statement to inform the participant that the survey complied with IRB requirements, (d) a statement that all information gathered would remain anonymous, and (e) a thank you note for participating in the survey.

Demographic Section

The demographics section (Section 1) included (a) instruction on completing the questionnaire and (b) questions that elicited the participant's demographic data. Critical in understanding human behavior is knowing how behavior varies across different groups or demographics (Nardi, 2003) because a person's behavior is influenced by cultures and

groups that develop their own values and norms over time (Karahanna et al., 2005). Collecting this information was important because earlier studies on the impact of such demographics as age and gender on computer usage may no longer be accurate (Knight & Pearson, 2005). According to Nardi (2003), questions about gender, race, age, income, education, and occupation are typical of demographic information. Because a user's behavior can be influenced by his or her demographic group membership, this study examined the influence of four demographic variables: gender, age, education, and occupation. A cross-reference matrix of Section 1 (the demographic section) to the survey instrument is provided in Table 1.

Table 1. Demographic Section (Section 1) Cross-Reference Matrix

Demographic (Population)	**Survey Question**	**Questionnaire Number**
Gender	Are you a female?	1
Age	Are you age 40 and over?	2
Education level	Are you a college graduate?	3
Occupation	Are you in a technical position?	4

To understand the participants' security behaviors, this study compared the results of the security questionnaire across the four demographics groups: gender (men vs. women), age (older participants vs. younger participants), education (college graduates vs. noncollege participants), and occupation (participants in technical positions vs. those in nontechnical positions).

Concerning the first demographic group of gender, Zukowski and Brown (2007) noted that women were more concerned about online security and privacy than their male

counterparts. This study assessed the gender group with the following question: Are female users more security aware?

In terms of the second demographic group, Zukowski and Brown (2007) stated that older users are more concerned about online security and privacy than their younger counterparts. For this study, older participants were defined as those aged 40 and over while younger participants were those aged 39 and younger. This study assessed the age group by seeking to answer the following question: Are users aged 40 and over more security aware?

Concerning the third demographic group of education, Zukowski and Brown (2007) indicated that individuals with lower levels of education may perform fewer online actions because of having greater concern about security than their counterparts with higher levels of education. For this study, lower levels of education were defined as not having attended college while higher levels of education were defined as having graduated from college. This study assessed the education group by answering the following question: Are users with higher levels of education more security aware?

Considering the fourth demographic group of occupation, Suchan (2003) stated that employees in technical positions or with technical backgrounds tended to violate or bypass security procedures more than their nontechnical counterparts. For this study, technical positions were defined as positions that required a college degree in engineering or information technology while nontechnical positions were defined as positions that did not require technical skills or abilities, such as logisticians and administrative personnel. This study assessed the occupation group by answering the following question: Are users in technical positions more security aware?

Security Section

The security section (Section 2) included (a) instruction on how to complete the questionnaire and (b) questions to gather the participants' security data. Security threats caused by users' inappropriate actions continue to be a significant security problem within any organization (Andrews & Whittaker, 2004; Blyth & Kovacich, 2006). Users must known when not to execute a dangerous e-mail attachment, when not to install online software, and when and how to take appropriate action when confronted with security threats (Aytes & Connolly, 2004). One way to lessen the impact of these security challenges is through information assurance training. Information security training not only raises user awareness levels but also provides users with the ability to recognize and prevent any inappropriate actions. A user's security awareness level was defined as whether a user would know whether an activity was wrong, would choose to report the misuse of the system, and would report a security incident. This section assessed whether the participants had been performing the simple everyday practices and behaviors necessary to avert insider threats. The security questionnaire was based on three security domains: (a) security training, (b) essential security practices, and (c) appropriate security actions. A cross-referenced matrix of the security section (Section 2) to the survey instrument is provided in Table 2.

Table 2. Security Section (Section 2) Cross-Reference Matrix

Survey Security Awareness	Survey Question	Questionnaire Number
Security Training	These questions ascertain the individual's security awareness training	1, 2
Essential Security Practices	These questions ascertain the proper/ essential security practices	3, 4
Appropriate Security Practices	These questions ascertain the proper security behavior/actions	5, 6, 7

The security training domain was addressed through two questions (Questions 1 and 2) that measured the participants' responses concerning security training and their ability to report security threats or virus alerts. Boyce and Jennings (2002) noted that, to prevent security threats, personnel need to participate in security training and know how to report security threats; that is, they should always participate in training and always report a security threat (Boyce & Jennings, 2002).

The essential security practices domain was investigated through two questions (Question 3 and 4) that measured the participants' responses concerning protecting their unattended systems and scanning e-mail attachments for viruses. Boyce and Jennings (2002) indicated that, to prevent unauthorized access, personnel need to protect their unattended systems by using a screen lock and scanning email attachments; that is, they should always secure their systems and scan attachments for viruses.

The appropriate security actions domain was addressed through three questions (Questions 5, 6 and 7) that measured the participants' responses concerning system security settings, access to their systems, and web downloads. Boyce and Jennings (2002) indicated that, to prevent unauthorized access, personnel need to disable the

automated password feature, prevent other people from accessing their systems, and avoid web downloading of applications; that is, they should never use the automated password feature, never provide others access to their systems, and never download web applications.

This entire section measured the participants' security behavior in order to answer the research question of whether there a relation between users' security behaviors and their levels of security awareness.

Measures

The survey instrument was designed in two sections having the following formats for collecting and measuring data on the participants:

- Demographic section (Section 1) used a binary (yes/no) format.
- Security section (Section 2) used a 5-point Likert scale (*Always*, *Sometimes*, *Neutral*, *Seldom*, and *Never*) to measure participants' security behaviors.

The Likert scale is a common scaling technique used for closed-ended survey research (Nardi, 2003). To complete the security questionnaire, participants were asked to place an "X" in the appropriate box to the right of each question. An example question from Section 2 is shown in Table 3.

Table 3. Security Section Example Question

	Always	Sometime	Neutral	Seldom	Never
1. Do you participate in security training?					

Data Collection

Data collection consisted of collecting the completed surveys and entering the data into a computer. The PM AAA Operations Officer collected and safeguarded the completed surveys (as indicated in Appendix C). Once collected, the responses were reviewed for usability. Partially completed questionnaires were considered unusable (Nardi, 2003). Responses from all usable questionnaires were entered in a Microsoft Excel spreadsheet. The collected surveys were kept in a secure location during the time the data were being entered. Afterward, the researcher destroyed all printed surveys.

Data Coding

The collected data were recorded in a Microsoft Excel spreadsheet. Because each participant indicated a response with an "X," when the data were recorded in the spreadsheet, the "X" was replaced with a "1" in order to tabulate all categorical data.

Format for Presenting the Results

Results of this study are presented in Chapter 4. Nardi (2004) stated that there are several ways of presenting data, including frequency tables, graphs or tables, and statistical significance. To determine statistical significance, social scientists have generally accepted that, if the probability value, symbolized by the lowercase *p*, is less than 5% ($p < .05$), the result is considered statistically significant (Nardi, 2003). For this study, a probability value of less than 5% was used. The *t* test was used to determine the statistical significance of the demographic data, and the Pearson chi-square was used to determine the statistical significance of the population's security data.

Resources Used

Resources required for this study included (a) a computer; (b) Microsoft Word for developing the survey instrument; (c) Microsoft Excel for recording the data, creating the frequency tables and bar graphs, and providing a statistical spreadsheet using the Excel chi-square and *t* test formulas; (d) a printer; (e) Internet access; and (f) access to PM AAA Intranet.

Summary

This chapter presented the methodology used for this study. The goal of the study was to determine whether the employees at a mid-sized research and manufacturing facility were engaging in proper information security behaviors and practices. Previous research that assessed the security behaviors of users had been conducted by Katz (2005). To measure the participants' security behavior, Katz used a 5-point Likert scale on a self-administered, closed-ended quantitative questionnaire. Because this study was a continuation of the work conducted by Katz, permission was obtained from him to adapt his methodology. This adaption was vital not only in maintaining the integrity of the baseline developed but also in providing a viable launching point for this study. This study's adaptation included replacing the physical/location questions with questions regarding security training. The demographic was expanded from faculty and staff to four demographic groups: gender, age, education, and occupation. Like that of Katz, this study used a self-administered, closed-ended questionnaire. The survey instrument used a binary scale to gather the participants' demographic data and a 5-point Likert scale to

measure the participants' security behaviors. The survey instrument was designed in three parts: (a) a cover letter, (b) a demographic section, and (c) a security section. The security questions were developed from three security domains: (a) security training, (b) essential security practices, and (c) appropriate security actions. The results of the survey are presented in Chapter 4, using frequency tables and bar graphs. The survey's results were analyzed using the following statistical tests: (a) demographic data were analyzed with a *t* test and (b) security behavior data were analyzed with the Pearson chi-square test. To determine whether the findings for both demographic groups and the participant population were statistically significant, a probability of less than 5% ($p < .05$) was used.

Chapter 4

Results

Background

This chapter presents the findings of this research study. The goal of this study was to determine the participants' behaviors and practices in information security. The study used a self-administered, closed-ended questionnaire to collect data on the demographic and research questions posed in the study. The findings are presented in frequency tables and graphs. Frequency tables show how each participant responded or scored on a given question (Nardi, 2003). Heiman (2006) stated that the most common way to organize scores is to create a simple frequency distribution, which shows the number of times each score occurs in a set of data. For this study, the frequency for each response or score is listed in raw numbers of occurrence and in percentages relative to the number of total responses (Nardi, 2003). According to Heiman (2006), presenting data in a graph or table is important for two reasons:

- First, it answers questions about the different scores that occurred in the data in an organized manner.
- Second, such presentations of data provide the building blocks for other descriptive and inferential statistics.

Findings

The survey instrument was designed in two sections: the first section focused on gathering the participants' demographic data while the second section focused on gathering information on the participants' security behaviors and practices. A total of 288 employees received the survey, and 92 returned the survey, with 87 or 30% completing the survey. The data in this study were taken from the 87 completed surveys. Responses to the survey were recorded and analyzed using a *t* test to determine the statistical significance between the demographic groups and a Pearson chi-square to determine the statistical significance of the participant's security responses.

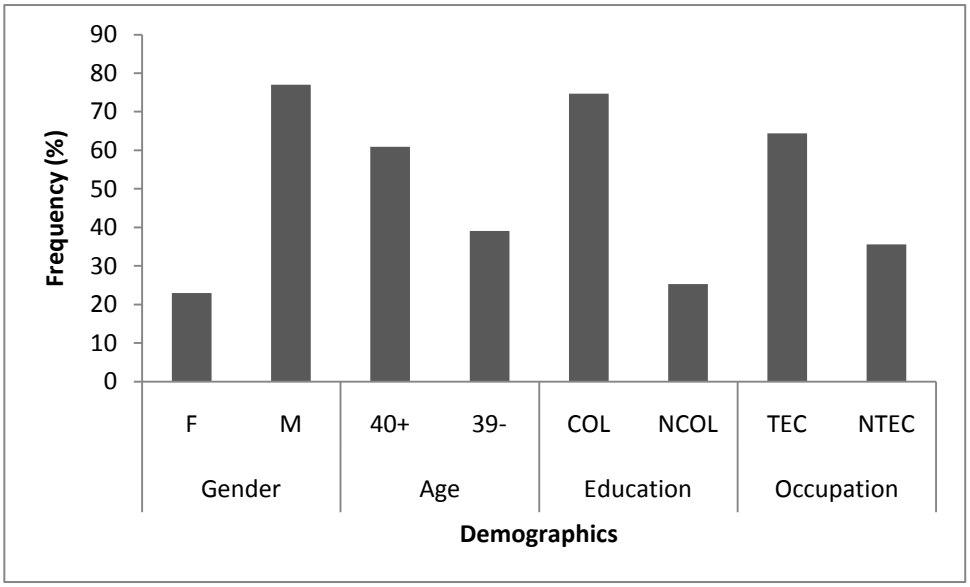
Demographics

This section presents the participants' responses to the survey's demographic questions. A binary (*yes*/*no*) scale was used to record the participants' responses. Table 4 shows the participants' responses in frequency and percentages. Figure 1 is a bar graph of the participants' responses in percentages. The results in terms of demographics are as follows:

- Gender: 77% of the participants indicated they were male.
- Age: 60.9% of the participants indicated they were age 40 or over.
- Education: 74.7% of the participants indicated they had attended college.
- Occupation: 64.4% of the participants indicated they were in a technical position.

Table 4. Demographic Data

Demographic Questions	Frequency		Percent	
	Yes	No	Yes	No
1. Are you a female?	20	67	23.0	77.0
2. Are you age 40 and over?	53	34	60.9	39.1
3. Are you a college graduate?	65	22	74.7	25.3
4. Are you in a technical position?	56	31	64.4	35.6



Legend:
F = Female, M = Male, 40+ = Age 40 & over, 39- = Age 39 & under, COL = College, NCOL = No College, TEC = Technical, NTEC = Nontechnical

Figure 1. Demographic data.

Security Survey

This section presents the participants' responses to the survey's security questions. A 5-point Likert scale was used to record the participants' responses as shown in Tables 5 to 11.

Security Question 1

Table 5 presents the participants' responses to Security Question 1: Do you participate in security training? According to the results, a majority (70.1%) of the sample population always participated in security training. The remaining responses included 11.5% indicating they sometimes participated in security training, 10.3% indicating they seldom participated in security training, 2.3% indicated they never participated in security training, and 5.7% remained neutral.

Table 5. Responses to Security Question 1

Likert scale	Frequency	Percent
Always	61	70.1
Sometimes	10	11.5
Neutral	5	5.7
Seldom	9	10.3
Never	2	2.3
Total	87	100.0

Security Question 2

Table 6 presents the participants' responses to Security Question 2: Do you know who to contact if you get a virus alert? According to the results, a majority (90.8%) of the sample population always knew who to contact if a security problem occurred. The remaining responses included 3.4% sometimes knowing who to contact, 3.4% never knowing who to contact, and 2.3% remained neutral concerning knowing who to contact if a security problem occurred.

Table 6. Responses to Security Question 2

Likert scale	Frequency	Percent
Always	79	90.8
Sometimes	3	3.4
Neutral	2	2.3
Seldom	0	0.0
Never	3	3.4
Total	87	100.0

Security Question 3

Table 7 presents the participants' responses to Security Question 3: Do you lock your screen or use a screen saver when you leave your computer? According to the results, a majority (65.5%) of the sample population always locked or used a screen saver when they left their computers. The remaining responses included 29.9% indicating they sometimes locked their screens, 2.3% indicating they seldom locked their screen, 1.1% indicating they never locked their screens, and 1.1% remaining neutral concerning locking their screens or using a screen saver when leaving their computers.

Table 7. Responses to Security Question 3

Likert scale	Frequency	Percent
Always	57	65.5
Sometimes	26	29.9
Neutral	1	1.1
Seldom	2	2.3
Never	1	1.1
Total	87	100.0

Security Question 4

Table 8 presents the participants' responses to Security Question 4: Do you scan all e-mail attachments for viruses? According to the results, under half (40.2%) of the sample population always scanned their e-mail attachments for viruses. The remaining responses included 10.3% indicating they sometimes scanned their e-mail attachments, 13.8% indicating they seldom scanned their e-mail attachments, 23% indicating they never scanned their e-mail attachments, and 12.6% remaining neutral concerning scanning their e-mail attachments for viruses.

Table 8. Responses to Security Question 4

Likert scale	Frequency	Percent
Always	35	40.2
Sometimes	9	10.3
Neutral	11	12.6
Seldom	12	13.8
Never	20	23.0
Total	87	100.0

Security Question 5

Table 9 presents the participants' responses to Security Question 5: Do you use the automatic save/remember password feature on your computer? This question was designed with a negative or *never* response. According to the results, under half (44.8%) of the sample population never used the automatic save/remember password feature. The remaining responses included 10.3% indicating they always used the save/remember

password feature, 21.8% indicating they sometimes used the save/remember password feature, 17.2% indicating they seldom used the save/remember password feature, and 5.7% remained neutral concerning using the automatic save/remember password feature.

Table 9. Responses to Security Question 5

Likert scale	Frequency	Percent
Always	9	10.3
Sometimes	19	21.8
Neutral	5	5.7
Seldom	15	17.2
Never	39	44.8
Total	87	100.0

Security Question 6

Table 10 presents the participants' responses to Security Question 6: Do other people have access or use of your computer? This question was designed with a negative or *never* response. According to the results, under half (46%) of the sample population never let other people have access to or use their computers. The remaining responses included 8% indicating they always let other people have access to or use of their computers, 18.4% indicating they sometimes let other people have access to or use of their computers, 20.7% indicating they seldom let other people have access to or use of their computers, and 6.9% remaining neutral concerning letting other people have access to or use of their computers.

Table 10. Responses to Security Question 6

Likert scale	Frequency	Percent
Always	7	8.0
Sometimes	16	18.4
Neutral	6	6.9
Seldom	18	20.7
Never	40	46.0
Total	87	100.0

Security Question 7

Table 11 presents the participants' responses to Security Question 7: Do you download anything from the web (e.g., applications, upgrades, music, video clips, etc.)? This question was designed with a negative or *never* response. According to the results, under half (48.3%) of the sample population never downloaded anything from the web. The remaining responses included 23% indicating they sometimes downloaded from the web, 27.6% indicating they seldom downloaded from the web, and 1.1% remained neutral concerning downloading from the web.

Table 11. Responses to Security Question 7

Likert scale	Frequency	Percent
Always	0	0.0
Sometimes	20	23.0
Neutral	1	1.1
Seldom	24	27.6
Never	42	48.3
Total	87	100.0

Analysis of Survey Questions

This section addresses the study's four demographic questions (DQ) and the research question (RQ). The survey questions were as follows:

DQ1: Are female users more security aware?

DQ2: Are users age 40 and over more security aware?

DQ3: Are users with higher levels of education more security aware?

DQ4: Are users in technical positions more security aware?

RQ: Is there a relationship between users' security behaviors and their levels of security awareness?

Data from the Likert scales can be simplified by either combining the response categories or reducing the results into nominal categories such as *agree*/*disagree* (Waikar & Huynh, 2008). Furthermore, Casper and Floyd (2009) indicated that the end point can be used as summated rating scales. For this study, the data from the Likert scales were simplified by reducing the following: (a) questions 1 through 4 used the *always* end point and (b) questions 5 through 7 used the *never* end point. The survey results were analyzed using the following statistical tests: (a) for demographic data, the *t* test was used, and (b) for security data, the Pearson chi-square test was used. To determine whether the findings for both the demographics and population were statistically significant, a probability of less than 5% ($p < .05$) was used.

Demographic Question 1 Gender Group

This section addressed the gender question: Are female users more security aware? The results of the security questionnaire by gender are presented in frequency and percentages in Table 12. The findings indicate how each group responded to each of the security questions. To address the gender question, the data were statistically analyzed using Microsoft's Excel TTEST (see Table 13).

Table 12. Security Responses by Gender

Security questions	Frequency		Percent	
	F (*n* = 20)	M (*n* = 67)	F	M
Q1	14	47	70.0	70.1
Q2	18	61	90.0	91.0
Q3	13	44	65.0	65.7
Q4	10	25	50.0	37.3
Q5	9	30	45.0	44.9
Q6	7	33	35.0	49.3
Q7	12	30	60.0	44.8

Note. The percentage is the frequency divided by the total participants multiplied by 100 (e.g., Q1 F = 14/20 x 100, M = 47/67 x 100).
F = female; M = male.

Results of the *t* test determined that the findings were statistically significant, thereby answering the question that female participants were more security aware than their male counterparts, as indicated in Table 13. In addition to answering the demographic question, the responses on the three security domains were analyzed to better understand where the security issues reside. Results of two of the three security domains, security training and appropriate security practices, were statistically significant, as shown in

Table 13. Female participants were overall more security aware; however, the results for the security domains indicate that males were more security aware in regards to security training while females were more security aware in regards to appropriate security practices. The findings also indicated that the participants' essential security practices and appropriate security practices were under 58%, indicating that each gender group had poor security practices.

Table 13. Security Analysis by Gender

Security domains	**Frequency**		**Percent**		***t* test**	
	F (*n* = 20)	**M (*n* = 67)**	**F**	**M**	***df***	**Sig.**
Gender total	11.9	38.6	59.3	57.6	6	8.59E-05*
Security training	16.0	54.0	80.0	80.6	1	0.01740*
Essential security practices	11.5	34.5	57.5	51.5	1	0.06962*
Appropriate security practices	9.3	31.0	46.7	46.3	2	0.00013*

Note. The percentage is the frequency divided by the total participants multiplied by 100.
F= female; M = male.
* $p < .05$ (one-tailed, two sample equal variance test).

Demographic Question 2 Age Group

This section addresses the age question: Are users age 40 and over more security aware? The results of the security questionnaire by age are presented in frequency and percentages in Table 14. The findings indicate how each group responded to each of the security questions. To address the age question, the data were statistically analyzed using Microsoft's Excel TTEST (see Table 15).

Table 14. Security Responses by Age

Security questions	Frequency		Percent	
	40+ (*n* = 53)	**< 40 (*n* = 34)**	**40+**	**< 40**
Q1	39	22	73.6	64.7
Q2	48	31	90.6	91.2
Q3	34	23	64.2	67.6
Q4	20	15	37.7	44.1
Q5	22	17	41.5	50.0
Q6	20	20	37.7	58.8
Q7	25	17	47.2	50.0

Note. The percentage is the frequency divided by the total participants multiplied by 100.
40+ = age 40 and over; < 40 = age 39 and under.

Results of the *t* test determined that the findings were statistically significant, thereby indicating that participants age 40 and over were not more security aware than their younger counterparts, as shown in Table 15. In addition to the age question, the responses to the three security domains were analyzed to better understand where the security issues reside. The results indicated that only one of the three security domains, appropriate security practices, was statistically significant, as shown in Table 15. Participants age 39 and younger were overall more security aware, including in terms of appropriate security practices. The findings also indicate that the participants' essential security practices and appropriate security practices was under 56%, indicating that each age group had poor security practices.

Table 15. Security Analysis by Age

Security domains	Frequency		Percent		*t* test	
	40+ (*n* = 53)	< 40 (*n* = 34)	40+	< 40	*df*	Sig.
Age total	29.7	20.7	56.1	60.9	6	0.036*
Security training	43.5	26.5	82.1	77.9	1	0.058 *
Essential security practices	27.0	19.0	50.9	55.9	1	0.213 *
Appropriate security practices	22.3	18.0	42.1	52.9	2	0.035 *

Note. The percentage is the frequency divided by the total participants multiplied by 100.
40+ = age 40 and over; < 40 = age 39 and under.
* $p < .05$ (one-tailed, two sample equal variance test).

Demographic Question 3 Education Group

This section addresses the education question: Are users with higher levels of education more security aware? The results of the security questionnaire by education are presented in frequency and percentages in Table 16. The findings indicate how each group responded to each of the security questions. To address the education question, the data were statistically analyzed using Microsoft's Excel TTEST, as shown in Table 17.

Table 16. Security Responses by Education

Security questions	Frequency		Percent	
	COL (*n* = 65)	NCOL (*n* = 22)	COL	NCOL
Q1	45	16	69.2	72.7
Q2	59	20	90.8	90.0
Q3	40	17	61.5	77.3
Q4	25	10	38.5	45.5
Q5	24	15	36.9	68.2
Q6	33	7	50.8	31.8
Q7	30	12	46.2	54.5

Note. Percentage is the frequency divided by the total participants multiplied by 100.
COL = college; NCOL = no college.

Results of the *t* test determined that the findings were statistically significant, thereby answering the question of whether participants with higher levels of education were more security aware than their noncollege counterparts (see Table 17). In addition to answering the education question, the data for the three security domains were analyzed to better understand where the security issues reside. The results indicate that two of the three security domains, security training and appropriate security practices, were statistically significant, as shown in Table 17. Noncollege participants were overall more security aware, including in terms of the security domains of security training and appropriate security practices. The findings also indicate that the participants' essential security practices and appropriate security practices were under 62%, indicating that each education group had poor security practices.

Table 17. Security Analysis by Education

Security domains	**Frequency**		**Percent**		***t* test**	
	COL (*n* = 65)	**NCOL (*n* = 22)**	**COL**	**NCOL**	***df***	**Sig.**
Education total	36.6	13.9	56.3	63.0	6	0.0006*
Security training	52.0	18.0	80.0	81.8	1	0.0214 *
Essential security practices	32.5	13.5	50.0	61.4	1	0.0742 *
Appropriate security practices	29.0	11.3	44.6	51.5	2	0.0037 *

Note. The percentage is the frequency divided by the total participants multiplied by 100.
COL = college; NCOL = no college.
* $p < .05$ (one-tailed, two sample equal variance test).

Demographic Question 4 Occupation Group

This section addresses the occupation question: Are users in a technical position more security aware? The results of the security questionnaire by occupation are presented in frequency and percentages in Table 18. The findings indicate how each group responded

to each of the security questions. To address the occupation question, the data were statistically analyzed using Microsoft's Excel TTEST (see Table 19).

Table 18. Security Responses by Occupation

Security questions	Frequency		Percent	
	TEC (*n* = 56)	NTEC (*n* = 31)	TEC	NTEC
Q1	36	25	64.3	80.6
Q2	53	25	94.6	83.9
Q3	36	21	64.3	67.7
Q4	22	13	39.3	41.9
Q5	25	14	44.6	45.2
Q6	21	19	37.5	61.3
Q7	25	17	44.6	54.8

Note. Percentage is the frequency divided by the total participants multiplied by 100. TEC = technical position; NTEC = nontechnical position.

Results of the *t* test determined that the findings were statistically significant, thereby answering the question of whether participants in technical positions were more security aware than those in nontechnical positions (see Table 19). In addition to answering the occupation question, the data for the three security domains were analyzed to better understand where the security issues reside. The results indicate that only one of the three security domains, appropriate security practices, was statistically significant, as shown in Table 19. Participants in nontechnical positions were, overall, more security aware, including in terms of appropriate security practices. The findings also indicate that the participants' essential security practices and appropriate security practices were under 55%, indicating that each occupation group had poor security practices.

Table 19. Security Analysis by Occupation

Security domains	Frequency		Percent		*t* test	
	TEC (*n* = 56)	NTEC (*n* = 31)	TEC	NTEC	*df*	Sig.
Occupational total	31.1	19.3	55.6	62.2	6	0.0138*
Security training	44.5	25.5	79.5	82.3	1	0.0770 *
Essential security practices	29.0	17.0	51.8	54.8	1	0.1370 *
Appropriate security practices	23.7	16.7	42.3	53.8	2	0.0110 *

Note. The percentage is the frequency divided by the total participants multiplied by 100.
TEC = technical position; NTEC = nontechnical position.
* $p < .05$ (one-tailed, two sample equal variance test).

Research Question

This section addresses the study's research question: Is there a relation between users' security behaviors and their levels of security awareness? The results of the security survey are presented in frequencies and percentages in Table 20. The findings indicate how participants responded to each of the security questions. To address the research question, the data were statistically analyzed using Microsoft Excel CHITEST (see Table 21).

Table 20. Security Responses by Population

Security questions	Population	
	Frequency	Percent
Q1	61	70.1
Q2	79	90.8
Q3	57	65.5
Q4	35	40.2
Q5	39	44.8
Q6	40	46.0
Q7	42	48.3

Note. Percentage is frequency divided by total participants multiplied by 100.
N = 87.

Results of the chi-square test determined that the findings were statistically significant, thereby answering the research question of whether there is a relation between users' security behaviors and their levels of security awareness (see Table 21). In addition to answering the research question, the data for the three security domains were analyzed to better understand where the security issues reside. The results indicate that only one of the three security domains, essential security practices, was statistically significant, as shown in Table 21. The findings also indicate that the participants' essential security practices and appropriate security practices were under 55%, indicating that the sample population had poor security practices.

Table 21. Security Analysis by Population

Security domains	**Population**		**Chi-square test**	
	Frequency	**Percent**	***df***	**Sig.**
Participant total	50.4	58.0	6	3.7E-05
Security training	70.0	80.5	1	0.1282 *
Essential security practices	46.0	52.9	1	0.0218 *
Appropriate security practices	40.3	46.4	2	0.9438 *

Note. The percentage is the frequency divided by the total participants multiplied by 100.
$N = 87$.
* $p < .05$.

Security Questions Range

This section presents the security results by the highest and lowest scores for each demographic group and total population (see Table 22). A break-down by security responses was conducted in order to understand where the security issues lay according to the sample population. Questions with high responses indicate strong security behaviors and practices while low responses indicate weak security behaviors and

practices. The findings indicate (see Table 22) that only one question received a consistently high response rate for each demographic group and the total population: Do you know who to contact if you get a virus alert? The results indicate that the participants had strong security behaviors and practices in regards to security training because they knew whom to contact if their systems had a security warning/alert. In addition, the findings indicate that the lowest response rate was shared among three security questions: (a) Question 4: Do you scan all email attachments for viruses? (b) Question 6: Do other people have access or use of your computer? (c) Question 5: Do you use the automatic save/remember password feature on your computer? (See Table 22.) The results indicate that the participants had weak security behaviors and practices in terms of scanning email attachments for viruses, allowing others access to or use of their systems, and using the system stored or saved password feature.

Summary

This chapter presented the results of this study. The goal was to measure the security behaviors of the sample population in order to determine the participants' security awareness levels. The data for this study were taken from 87 surveys completed by the sample population. The survey responses were used to address the study's four demographic questions (DQ) and its research question (RQ): (a) DQ1: Are female users more security aware? (b) DQ2: Are users age 40 and over more security aware? (c) DQ3: Are users with higher levels of education more security aware? (d) DQ4: Are users in technical positions more security aware? (e) RQ: Is there a relation between users' security behaviors and their levels of security awareness?

Table 22. Security Questions Range

Demographic Group	High range		Low range	
	SEC-Q	Percent	SEC-Q	Percent
Gender				
F	Q-2	91.0	Q-4	37.3
M	Q-2	90.0	Q-6	35.0
Age				
40+	Q-2	90.6	* Q-4/Q-6	37.7
< 40	Q-2	91.2	Q-4	44.1
Education				
COL	Q-2	90.8	Q-5	36.9
NCOL	Q-2	90.9	Q-6	31.8
Occupation				
TEC	Q-2	94.6	Q-6	37.5
NTEC	Q-2	83.9	Q-4	41.9
Population	Q-2	90.8	Q-4	40.2

F = female, M = male; 40+ = age 40 and over, > 40 = age 39 and under; COL = college, NCOL = No college; TEC = technical position, NTEC = nontechnical position.
* Questions that had the same responses.

To answer the study's questions the results were analyzed using the following statistical tests: (a) the *t* test for the demographic data, and (b) the Pearson chi-square test for the security behavior data. To determine whether the findings for both the demographics and population were statistically significant, a probability of less than 5% ($p < .05$) was used. The results determined the following: (a) DQ1 findings were statistically significant, thereby answering the question of whether female participants were more security aware than their male counterparts. (b) DQ2 findings were statistically significant, thereby answering the question of whether participants age 40 and over were more security aware than their younger counterparts. (c) DQ3 findings were statistically significant, thereby answering the question of whether participants with

higher levels of education were more security aware than their noncollege counterparts. (d) DQ4 findings were statistically significant, thereby answering the question of whether participants in technical positions were more security aware than their nontechnical counterparts. (e) RQ findings were statistically significant, thereby answering the research question of whether there is a relation between users' security behaviors and their levels of security awareness.

The study also compared the security results by the highest and lowest scores for each demographic group and total population. The findings indicate that one question, Question 2, consistently had a high response rate by each demographic group and the total population: Do you know who to contact if you get a virus alert? The results determined that the participants had strong security behaviors and practices in regards to security training because they knew who to contact if their systems displayed a security warning/alert. In addition, the findings indicate that the lowest response rate was shared across three security questions: (a) Q4 Do you scan all email attachments for viruses? (b) Q6 Do other people have access or use of your computer? (c) Q5 Do you use the automatic save/remember password feature on your computer? The results determined that the participants had weak security behaviors and practices in regards to scanning email attachments for viruses, allowing others access to or use of their systems, and using the system stored/saved password feature.

Chapter 5

Conclusions, Implications, Recommendations, and Summary

Conclusion

The goal of this study was to determine whether employees were engaging in proper information security behavior and practices. Doing so was accomplished by measuring participants' security behaviors and practices using a 5-point Likert scale in a self-administered, closed-ended, quantitative questionnaire. The sample population consisted of working professionals at a mid-sized research and manufacturing facility in northern Virginia. The response rate for this study was 30%. The participants' responses were used to answer the study's four demographic questions and the research question. The data were analyzed using the following statistical analysis tools: Demographic data were analyzed using a *t* test, and population security data were analyzed using the Pearson chi-square. To determine whether the findings were statistically significant for both the demographic groups and the entire population, a probability of less than 5% ($p < .05$) was used.

The first demographic question was as follows: Are female users more security aware? The results were statistically significant, indicating that females were more security aware than their male counterparts. To better understand where the security issues resided, the results were analyzed according to the three security domains. The findings indicated that responses for two of the three security domains were statistically

significant: security training and appropriate security practices. Although female participants were generally more security aware, results by the security domains indicated that male participants were more security aware in regards to security training while female participants were more security aware in regards to appropriate security practices.

The second demographic question was as follows: Are users age 40 and over more security aware? The results were statistically significant, indicating that participants age 39 and younger were more security aware than their counterparts age 40 and over. To better understand where the security issues resided, the results were analyzed according to the three security domains. The findings indicated that the responses for only one of the three security domains were statistically significant: appropriate security practices. Younger participants were more security aware not only in general but also in the security domain.

The third demographic question was the following: Are users with higher levels of education more security aware? The results were statistically significant, indicating that participants who did not attend college (noncollege) were more security aware than their higher educated counterparts. To better understand where the security issues resided, the results were analyzed according to the three security domains. The findings indicated that responses concerning two of the three security domains were statistically significant: security training and appropriate security practices. Noncollege participants were more security aware in general and, specifically, in those two security domains than those without higher education.

The fourth demographic question was as follows: Are users in a technical position more security aware? The results were statistically significant, indicating that

participants in nontechnical positions were more security aware than their counterparts in technical positions. To better understand where the security issues resided, the results were analyzed according to the three security domains. The findings indicated that only one of the three security domains was statistically significant: appropriate security practices.

The following research question guided this study: Is there a relation between users' security behaviors and their levels of security awareness? The results were statistically significant, indicating that a relation exists between users' security behaviors and their levels of security awareness.

In order to understand where the differences among security issues lay for the total population, the results were reviewed according to security responses. This review resulted in identifying the highest and lowest scores for each demographic group and the total population. The security question receiving the highest responses from each demographic group and the total population was Question 2: Do you know who to contact if you get a virus alert? The responses indicated that the participants know who to contact if they receive a virus alert. Three security questions received the lowest responses from each demographic group and the total population: (a) Question 4: Do you scan all email attachments for viruses? (b) Question 6: Do other people have access or use of your computer? (c) Question 5: Do you use the automatic save/remember password feature on your computer? These results indicated that the participants had weak security behaviors and practices in regards to scanning email attachments, allowing others to have access to their systems, and using the stored/saved password feature on their system.

Implications

This study has a number of implications concerning individuals' security practices and behaviors. First, results of the survey indicated that younger participants were more security aware than their older counterparts. This finding challenges the results of the literature review that older individuals are more concerned about security than their younger counterparts. Second, results for the research question indicated that a relation exists between individuals' security behaviors and their levels of security awareness; however, the overall response rate of the sample population was 58%, indicating that 42% of the population engages in inappropriate security practices and behaviors.

Furthermore, the low responses for the security questions indicated the following: (a) 40.2% of the participants always scanned their email attachments for viruses while 58.2% do not, making their systems vulnerable to a virus attack; (b) 40.6% of the participants never allowed others access to their system while 59.4% allowed others access to their system, making their systems or the data on their systems vulnerable to compromise; and (c) 44.8% of the participants never used the automatic/save password feature while 55.2% used the feature, leaving their systems' passwords vulnerable to being compromised. These results indicate that the participants were either ignoring their training by engaging in poor security practices or the security training provided did not raise their security awareness level enough to prevent such poor practices.

The results of this study will enhance the existing body of security knowledge by providing the security community with a better understanding of individuals' security practices and behaviors. These results could be used in developing ways to reduce the

inappropriate user actions, thereby increasing organizations' and individuals' information security.

Recommendations

Results of this study make it clear that further research is needed. Areas for future research include assessing individuals' security practices and behaviors in other organization or business environments. Moreover, because the results of the study challenged the literature by indicating that younger employees were more security aware than older employees, an effort should be made to verify the results of this study. Another area for further research is that of assessing organizations' security training to determine whether training improves the awareness levels of individuals. These recommendations can be used to avert the inappropriate user actions and reduce the number of internal security threats.

Summary

Threats to information security are constantly growing and vary from organization to organization, but the one threat that remains the same, regardless of the type of organization, is the insider security threat (Carroll, 2006). Insider security threats resulting from poor judgment or inappropriate actions by a user continue to be a significant security problem within all types of organizations (Aytes & Connolly, 2004). Inappropriate actions include any of the following: (a) leaving a laptop or sensitive document unattended, (b) inadvertently installing a virus from an e-mail attachment, (c) downloading unauthorized software, (d) reconfiguring a workstation's security setting,

(e) disabling a firewall, (f) providing personal information, or (g) failing to protect a password (Blyth & Kovacich, 2006). Insider threats may not occur as frequently as external attacks, but they have a higher rate of success, can go undetected, and pose a greater risk than an external attack (Chinchani et al., 2005). These internal threats continue to pose a significant security challenge within any organization. One way to lessen the impact of these security challenges is through information assurance training. Information assurance training not only raises users' awareness levels but also provides users with the ability to recognize and prevent any inappropriate actions. However, prior to conducting any security training, an organization security manager must assess the organization's state of security awareness (Blyth & Kovacich, 2006).

The purpose of this study was to assess the security behaviors and practices of common system users. Previous research in assessing the security behavior of a user had been conducted by Katz (2005). To measure the participants' security behavior, Katz used a 5-point Likert scale in a self-administered, closed-ended quantitative questionnaire. Because this study was a continuation of the work conducted by Katz, permission was obtained from Katz to adapt his methodology. This adaptation included replacing the physical and location questions with questions regarding security training. Because a user's behavior can be influenced by demographic groups, this adaptation also included examining the influence on the security behavior of four demographic groups: gender, age, education, and occupation. This survey instrument was designed in two sections: the demographic section, which used a binary scale to gather the participants' demographic data, and a security section, which used a 5-point Likert scale to measure the participants' security behavior.

Eighty-seven of the 288 employees at the General Dynamic and Program Manager Advanced Amphibious Assault (GD & PM AAA) Facility in Woodbridge, Virginia, completed the survey for a return rate of 30%. Results of this study were based on those completed surveys. The participants' responses were used to answer four demographic questions concerning gender, age, education, and occupation and the research question. The demographic data were analyzed using a *t* test, and the population security data were analyzed using the Pearson chi-square test. To determine whether the findings were statistically significant for specific demographic groups and the population as a whole, a probability of less than 5% ($p < .05$) was used.

The results for the gender demographic group were statistically significant, indicating that females were more security aware than their male counterparts. The results for the age demographic group were also statistically significant, indicating that participants aged 39 or younger were more security aware than their older counterparts aged 40 or more. Furthermore, for the education demographic group, the results were again statistically significant, indicating that participants who had not attended college were more security aware than their higher educated counterparts. In addition, the results for the demographic group classified as to position type were statistically significant, indicating that participants in nontechnical positions were more security aware than those who were in technical positions. Finally, the results addressing the research question were also statistically significant, indicating that a relation exists between users' security behaviors and their levels of security awareness.

A review of security items on the survey that received the highest and lowest scores for demographic groups and the total population indicated the following. The

participants knew whom to contact if they received a virus alert. However, only 40.2% of the participants always scanned their email attachments for viruses while 58.2% did not, leaving their systems vulnerable to a virus attack. In addition, 40.6% of the participants never allowed others access to their system while 59.4% did so, making their systems or the data on their systems vulnerable to compromised. Finally, 44.8% of the participants never used the automatic/save password feature on their computers while 55.2% did use the feature, leaving their system passwords vulnerable to compromise.

In conclusion, the results indicated that the gender, occupation, and education demographics confirmed the literature findings; however, the age demographic indicated that younger participants were more security aware, disputing the literature that stated that older participants were more security aware. Although the research question indicated that a relation between individuals' security behavior and their level of security awareness exists, the overall response rate of the sample population was 58%, indicating that 42% of the population was engaging in inappropriate security practices and behavior. These results imply that the participants are either ignoring their training by engaging in poor security practices or the security training provided did not raise their security-awareness level to prevent such poor practices.

Appendix A

Certificate of Authorship of Dissertation Work

NOVA SOUTHEASTERN UNIVERSITY
The Graduate School of Computer and Information Sciences

Certification of Authorship of Dissertation Work

Submitted to (Advisor's Name): Dr. William Hafner

Student's Name: Gordon J. Grant

Date of Submission: 26 May 2010

Purpose and Title of Submission: Dissertation Report
Ascertaining the Relationship between Security Awareness and the Security Behavior of Individuals

Certification of Authorship: I hereby certify that I am the author of this document and that any assistance I received in its preparation is fully acknowledged and disclosed in the document. I have also cited all sources from which I obtained data, ideas, or words that are copied directly or paraphrased in the document. Sources are properly credited according to accepted standards for professional publications. I also certify that this paper was prepared by me for this purpose.

Student's Signature: Gordon J. Grant

Appendix B

Permission to Use Survey

From: Frank Katz [mailto:Frank.Katz@armstrong.edu]
Sent: Monday, February 16, 2009 3:43 PM
To: Grant, Gordon (Cont)
Subject: Re: permission to use survey

I hereby give Gordon J. Grant permission to use my paper, "The Effect of a University Information Security Survey on Instruction Methods in Information Security," published in the Digital Library of the ACM and published and presented at InfosecCD 2005, in his doctoral research.

Sincerely,
Frank H. Katz

Frank H. Katz
Assistant Professor
Department of Information Technology
Armstrong Atlantic State University
912-344-3192

>>> "Grant, Gordon (Cont)" <gjgrant@egginc.com> 2/16/2009 3:27 PM >>>
Prof Katz,

This is a following-up, per our phone conversation today 16 Feb 09 at 3:21 PM regarding your granting me permission to use your survey for my dissertation. I need an email response to place in my dissertation.

Thank you,

RS
Gordon J. Grant
gjgrant@egginc.com
703-445-3462

From: Grant, Gordon (Cont)
Sent: Tuesday, October 07, 2008 10:51 AM
To: 'Frank.Katz@armstrong.edu'
Cc: Grant, Gordon (Cont)
Subject: Permission to use survey
Importance: High

Professor Katz,

My dissertation is similar to the study you conducted and presented at the InfoSecCD Conference in September 2005. Instead of surveying an academic environment I will be surveying a research/manufacturing environment. I am therefore requesting permission to use your survey as part of my dissertation.

RS
Gordon J. Grant
PhD candidate
Nova Southeastern University
703-441-7071
gjgrant@egginc.com
grantg@nsu.nova.edu

Appendix C

Officials Granting Permission to Conduct the Investigation

Grant, Gordon (Cont)

From: OBrien Maj William E
Sent: Thursday, September 11, 2008 2:48 PM
To: Grant CTR Gordon J
Subject: RE: Conduct PhD Survey

Mr. Grant,

Col Moore has authorized the Advanced Amphibious Assault program office to participate in your survey. This is strictly on a volunteer basis and will be contained only on the government side to include contractors that are in direct support of government functions. Your initial solicitation will be via e-mail with the attached survey form for individuals to print out, answer the questions then return to myself. I will collect these forms then immediate place them in my government safe until the deadline for submission has passed. I will then place the completed surveys into one envelope and provide them to you.

I am still working the total number of personnel here that will be provided the opportunity to participate in your survey.

r/

Maj O'Brien
703 492 3308

-----Original Message-----
From: Grant CTR Gordon J
Sent: Tuesday, August 19, 2008 11:09 AM
To: OBrien Maj William E
Cc: Grant CTR Gordon J; 'gjgrant@egginc.com'
Subject: Conduct PhD Survey

Maj O'Brien

As per our conversation on Thursday 7 August at the Clubs at Quantico enclosed is what we discussed.

I am a contractor supporting System Engineering (SE) and a PhD student at Nova Southeastern University (NSU). The purpose of my dissertation is to evaluate the information security behavior of individuals. The intent is to take a snapshot of the current information assurance awareness practices of the common user within PM AAA and General Dynamics facility. The results of this survey will provide academic and security community with a means of assessing and developing better ways in preventing security threats.

To do this I would like to e-mail my survey to everyone in the command intranet. Because this research is with human subjects prior to being able to submit my survey it will have to be reviewed and approved by PM AAA and my schools (NSU) Institutional Review Board (IRB). If PM AAA has an IRB representative they would also have to review the survey prior to submission.

I am therefore requesting permission to conduct my survey via the PM AAA intranet.

Enclosed is a copy of the survey for your review. If there are any questions or problems feel free to contact me.

RS
Gordon Grant
Principal System Engineer
Alion Science & Technology/EG&G CEOss Team
703-441-7071
gjgrant@egginc.com
grantgj.ctr@efv.usmc.mil
ggrant@alionscience.com

Note: (FYI)
The IRB is a federal regulation that protects the rights and privacy of human subjects involved in research activities. The National Research Act Public Law 99-158, the Health Research Extension Act of 9185, and the National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research provide guidelines for research with human subjects to ensure their protection in the design and conduct of research. These federal regulations require that any institution requesting and receiving funds from a federal department or agency for research involving human subjects must assure that such research is reviewed and approved by the institution's IRB.

Appendix D

IRB Approval

NOVA SOUTHEASTERN UNIVERSITY
Office of Grants and Contracts
Institutional Review Board

MEMORANDUM

To: Gordon Grant

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

Date: Jan. 29, 2009

Re: *Ascertaining the Relationship between Security Awareness and the Security Behavior of Individuals*

IRB Approval Number: wang11150801

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

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

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

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

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

Cc: Protocol File

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

Appendix E

Survey Instrument

INFORMATION ASSURANCE QUESTIONNAIRE

My name is Gordon Grant and I am a PhD candidate at Nova Southeastern University (NSU) Graduate School of Computer and Information Sciences. By completing this survey you will assist me with my dissertation which is dedicated in evaluating information assurance practices. The intent of this survey is to take a snapshot of the current information assurance practices within your organization. The results of this survey will provide academic and security researchers with the means of assessing and developing better ways in preventing unintentional security threats that can lead to identity theft.

This survey is constructed in two sections: demographics (section-1), and security (section-2). This survey should only take 2 minutes to complete. In keeping with NSU Institutional Review Board (IRB) requirements, at no time will any identifying information be asked of you or be given out. All information provided will be kept strictly confidential and any identifying information on the questionnaire will be discarded upon receipt. The results of this survey will be presented as percentages or graphs.

Please answer each question candidly and submit the completed survey with this cover sheet to the Operations Officer (Major O'Brien). Refer all questions to: grantg@nsu.nova.edu or gjgrant@egginc.com

Consent statement:

[ ] I consent to participate in this study.
(*please check*)

Thank you for your assistance.

SECTION – 1

DEMOGRAPHICS

Instructions:

1. This section will gather demographic information (e.g., gender, age, education, and occupation) from each participant which will be used to set up the variables for the statistical analysis.
2. Please place an "X" in the appropriate column box located to the right of the question.

Explanation of the questions:

1. Question 1: self explanatory
2. Question 2: self explanatory
3. Question 3: a "Yes" indicates that you attended or received a college diploma or degree
4. Question 4: self explanatory

Please check the box that describes you:

	Yes	No
1. Are you a female?		
2. Are you age 40 and over?		
3. Are you a college graduate?		
4. Are you in a technical position?		

SECTION – 2

SECURITY QUESTIONS

Instructions:

1. Please read through the following explanations to understand each choice on the questionnaire.
    a. **Always** is when you perform the action all the time
    b. **Sometimes** is when you performed the action several times a week
    c. **Neutral** is when you do not understand the question, you are unsure about how to answer the question, the question does not apply or you do not want to answer the question
    d. **Seldom** is when you performed the action once a month
    e. **Never** you do not performed this action

2. Then place an "X" in the box to the right of the question that most closely describes your actions.

3. Remember to answer every question candidly. There are no "right" or "wrong" answers, this survey is to get a better idea on current computer security practices.

4. All information will be kept confidential; any identifying information will be discarded upon receipt.

Section – 2

SECURITY QUESTIONS

Please check the appropriate box that most closely describes your actions:

	Always	Sometime	Neutral	Seldom	Never
1. Do you participate in security training?					
2. Do you know who to contact if you get a virus alert?					
3. Do you lock your screen or use a screensaver when you leave your computer?					
4. Do you scan all e-mail attachments for viruses?					
5. Do you use the automatic save/remember password feature on your computer?					
6. Do other people have access or use of your computer?					
7. Do you download anything from the web (e.g., applications, upgrades, music, video clips, etc.)?					

Thank you for participating in this survey.

Please return the completed questionnaire to Major O'Brien

Appendix F

Raw Data

Raw Data
Section-1 Demographics Questionnaire

Table F1. Demographic Responses.

1. Gender	Yes	No
Are you a female?	20	67

2. Age	Yes	No
Are you age 40 and over?	53	34

3. Education	Yes	No
Are you a college graduate?	65	22

4. Occupation	Yes	No
Are you in a technical position?	56	31

Raw Data
Section-2 Security Questionnaire

Table F2. Security Responses by Sample Population.

	Always	Sometime	Neutral	Seldom	Never
1. Do you participate in security training?	61	10	5	9	2
2. Do you know who to contact if you get a virus alert?	79	3	2	0	3
3. Do you lock your screen or use a screen saver when you leave your computer?	57	26	1	2	1
4. Do you scan all e-mail attachments for viruses?	35	9	11	12	20
5. Do you use the automatic save/remember password feature on your computer?	9	19	5	15	39
6. Do other people have access or use of your computer?	7	16	6	18	40
7. Do you download anything from the web (e.g., applications, upgrades, music, video clips, etc.)?	0	20	1	24	42

Table F3. Security Responses by Gender (Female/Male).

	Always	Sometime	Neutral	Seldom	Never
1. Do you participate in security training?					
Female	14	2	2	2	0
Male	47	8	3	7	2
2. Do you know who to contact if you get a virus alert?					
Female	18	0	1	0	1
Male	61	3	1	0	2
3. Do you lock your screen or use a screen saver when you leave your computer?					
Female	13	7	0	0	0
Male	44	19	1	2	1
4. Do you scan all e-mail attachments for viruses?					
Female	10	2	1	1	6
Male	25	7	10	11	14
5. Do you use the automatic save/remember password feature on your computer?					
Female	3	4	0	4	9
Male	6	15	5	11	30
6. Do other people have access or use of your computer?					
Female	2	2	0	9	7
Male	5	14	6	9	33
7. Do you download anything from the web (e.g., applications, upgrades, music, video clips, etc.)?					
Female	0	5	0	3	12
Male	0	15	1	21	30

Table F4. Security Responses by Age (40 & over/39 & under).

	Always	Sometime	Neutral	Seldom	Never
1. Do you participate in security training?					
Age 40 & Over	39	4	5	3	2
Age 39 & Under	22	6	0	6	0
2. Do you know who to contact if you get a virus alert?					
Age 40 & Over	48	2	2	0	1
Age 39 & Under	31	1	0	0	2
3. Do you lock your screen or use a screen saver when you leave your computer?					
Age 40 & Over	34	17	1	0	1
Age 39 & Under	23	9	0	2	0
4. Do you scan all e-mail attachments for viruses?					
Age 40 & Over	20	5	6	8	14
Age 39 & Under	15	4	5	4	6
5. Do you use the automatic save/remember password feature on your computer?					
Age 40 & Over	8	13	2	8	22
Age 39 & Under	1	6	3	7	17
6. Do other people have access or use of your computer?					
Age 40 & Over	4	12	3	14	20
Age 39 & Under	3	4	3	4	20
7. Do you download anything from the web (e.g., applications, upgrades, music, video clips, etc.)?					
Age 40 & Over	0	14	1	13	25
Age 39 & Under	0	6	0	11	17

Table F5. Security Responses by Education (College/No-College).

	Always	Sometime	Neutral	Seldom	Never
1. Do you participate in security training?					
College	45	6	5	8	1
No-College	16	4	0	1	1
2. Do you know who to contact if you get a virus alert?					
College	59	2	2	0	2
No-College	20	1	0	0	1
3. Do you lock your screen or use a screen saver when you leave your computer?					
College	40	21	1	2	1
No-College	17	5	0	0	0
4. Do you scan all e-mail attachments for viruses?					
College	25	6	7	10	17
No-College	10	3	4	2	3
5. Do you use the automatic save/remember password feature on your computer?					
College	9	17	1	14	24
No-College	0	2	4	1	15
6. Do other people have access or use of your computer?					
College	4	11	6	11	33
No-College	3	5	0	7	7
7. Do you download anything from the web (e.g., applications, upgrades, music, video clips, etc.)?					
College	0	14	1	20	30
No-College	0	6	0	4	12

Table F6. Security Responses by Occupation (Technical/Nontechnical).

	Always	Sometime	Neutral	Seldom	Never
1. Do you participate in security training?					
Technical	36	7	5	6	2
Nontechnical	25	3	0	3	0
2. Do you know who to contact if you get a virus alert?					
Technical	53	1	1	0	1
Nontechnical	26	2	1	0	2
3. Do you lock your screen or use a screen saver when you leave your computer?					
Technical	36	17	1	1	1
Nontechnical	21	9	0	1	0
4. Do you scan all e-mail attachments for viruses?					
Technical	22	5	10	8	11
Nontechnical	13	4	1	4	9
5. Do you use the automatic save/remember password feature on your computer?					
Technical	5	16	2	8	25
Nontechnical	4	3	3	7	14
6. Do other people have access or use of your computer?					
Technical	5	11	5	14	21
Nontechnical	2	5	1	4	19
7. Do you download anything from the web (e.g., applications, upgrades, music, video clips, etc.)?					
Technical	0	13	1	17	25
Nontechnical	0	7	0	7	17

Reference List

Al-Hamdani, W. A. (2006). Assessment of need and method of delivery for information security awareness program. *ACM Proceedings of the 3rd Annual Conference on Information Security Curriculum Development 2006 (InfoSecCD 06)*, Kennesaw, Georgia, 102-108.

Andrews, M., & Whittaker, J. A. (2004). Computer security. *IEEE Security & Privacy, 2*(5), 68-71.

Arce, I. (2003). The weakest link revisited. *IEEE Security & Privacy, 1*(2), 72-76.

Arce, I. (2004). More bang for the bug: An account of 2003's attack trends. *IEEE Security & Privacy, 2*(1), 66-68.

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

Balfanz, D., Durfee, G., Smetters, D. K., & Grinter, R. E. (2004). In search of usable security: Five lessons from the field. *IEEE Security & Privacy, 2*(5), 19-24.

Bishop, M., & Frincke, D. (2005). A human endeavor: Lessons from Shakespeare and beyond. *IEEE Security & Privacy, 3*(4), 49-51.

Blyth, A., & Kovacich, G. (2006). *Information assurance: Security in the information environment* (2nd ed.). Cambridge, MA: Springer.

Boyce, J., & Jennings, D. (2002). *Information assurance: Managing organizational IT security risks*. Woburn, MA: Butterworth-Heinemann.

Bradley, J., & Lee, C. C. (2007). ERP training and user satisfaction: A case study. *International Journal of Enterprise Information Systems, 3*(4), 33-50.

Campbell, P., Calvert, B., & Boswell, S. (2003). *Security+ guide to network security fundamentals*. Boston, MA: Thomson Course Technology.

Carroll, M. D. (2006). Information security: Examining and managing the insider threat. *ACM Proceedings of the 3rd Annual Conference on Information Security Curriculum Development 2006 (InfoSecCD 06)*, Kennesaw, Georgia, 156-158.

Casper, J. M., & Floyd, M. F. (2009). A comparison of end-point only versus fully-verbal labeled response scales. *2009 North American Society for Sport Management Conference (NASSM 2009)*, Columbia, SC, 355-356.

Chinchani, R., Iyer, A., Ngo, H. Q., & Upadhyaya, S. (2005). Towards a theory of insider threat assessment. *IEEE Proceedings of the 2005 International Conference on Dependable Systems and Networks (DSN 05)*, Yokohama, Japan, 108-117.

Conti, G., & Sobiesk, E. (2007). An honest man has nothing to fear: User perceptions on web-based information disclosure. *ACM Proceedings of the 3rd Symposium on Usable Privacy and Security 2007 (SOUPS 07)*, Pittsburgh, PA, 112-121.

Cranor, L. F., & Garfinkel, S. (2004). Editor's introduction: Secure or usable. *IEEE Security & Privacy, 2*(5), 16-18.

Creswell, J. (2003). *Research design: Qualitative, quantitative, and mixed methods approaches* (2nd ed.). Thousand Oaks, CA: Sage.

Crossler, R. E., & Belanger, F. (2006). The effect of computer self-efficacy on security training effectiveness. *ACM Proceedings of the 3rd Annual Conference on Information Security Curriculum Development 2006 (InfoSecCD 06)*, Kennesaw, Georgia, 124-129.

Dark, M., Harter, N., Morales, L., & Garcia, M. A. (2008). An information security ethics education model. *ACM Journal of Computing Sciences in Colleges (CSC), 23*(6), 82-88.

Dean, T. (2003). *Guide to telecommunications technology*. Boston, MA: Thompson Course Technology.

Dhamija, R., Tygar, J. D., & Hearst, M. (2006). Why phishing works. *ACM Proceedings of the SIGCHI Conference on Human Factors in Computing Systems 2006*, Montreal, Quebec, Canada, 581-590.

Dhillon, H., & Hentea, M. (2005). Getting a cybersecurity program started on low budget. *ACM Proceedings of the 43rd Annual Southeast Region Conference – Volume 1*, Kennesaw, GA, 294-300.

Doherty, N. F., & Fulford, H. (2005). Do information security policies reduce the incidence of security breaches: An exploratory analysis. *Information Resources Management Journal, 18*(4), 21-39.

Engelman, S., Cranor, L. F., & Hong, J. (2008). You've been warned: An empirical study of the effectiveness of web browsing phishing warnings. *ACM Proceedings of the 26th Annual SIGCHI Conference on Human Factors in Computing Systems 2008*, Florence, Italy, 1065-1074.

Gaw, S., Felten, E. W., & Fernandez-Kelly, P. (2006). Secrecy, flagging, and paranoia: Adoption criteria in encrypted e-mail. *ACM Proceedings of the Annual SIGCHI Conference on Human Factors in Computing Systems 2006*, Montreal, Quebec, Canada, 591-600.

Gross, J. B., & Rosson, M. B. (2007a). Looking for trouble: understanding end user security management. *ACM Proceedings of the 2007 Symposium on Computer Human Interaction for the Management of Information Technology (CHIMIT 07)*, Cambridge, MA, article 10.

Gross, J. B., & Rosson, M. B. (2007b). End user concern about security and privacy threats. *ACM Proceedings of the 3rd Symposium on Usable Privacy and Security 2007 (SOUPS 07)*, Pittsburgh, PA, 167-168.

Havana, T., & Roning, J. (2004). Attitudes and perceptions related to information security case: Rotuaari. *IEEE Proceedings of the 30th EUROMICRO Conference*, Rennes, France, 538-543.

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

Heiman, G. W. (2006). *Basic statistics for the behavioral sciences* (5th ed.). Boston, MA: Houghton Mifflin.

Herrmann, D. (2002). *A practical guide to security engineering and information assurance*. Boca Raton, FL: CRC Press.

Herzog, A., & Shahmehri, N. (2007). User help techniques for usable security. *ACM Proceedings of the 2007 Symposium on Computer Human Interaction for the Management of Information Technology (CHIMIT 07)*, Cambridge, MA, article 11.

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

Jakobsson, M., Stolterman, E., Wetzel, S., & Yang, L. (2008). Love of authentication. *ACM Proceedings of the 26th Annual SIGCHI Conference on Human Factors in Computing Systems 2008*, Florence, Italy, 197-200.

John, M., Maurer, F., & Tessem, B. (2005). Human and social factors of software engineering workshop summary. *ACM SIGSOFT Software Engineering Notes, 30*(4), 1-6.

Jungck, P., & Shim, S. S. (2004). Issues in high-speed Internet security. *IEEE Computer, 37*(7), 36-42.

Karahanna, E., Evaristo, J. R., & Srite, M. (2005). Levels of cultural and individual behavior: An investigative perspective. *Journal of Global Information Management, 13*(2), 1-20.

Katz, F. H. (2005). The effect of a university information security survey on instruction methods in information security. *ACM Proceedings of the 2nd Annual Conference on Information Security Curriculum Development (InfoSecCD)*, Kennesaw, GA, 43-48.

Kemmerer, R. A. (2003). Cybersecurity. *IEEE Proceedings of the 25th International Conference of Software Engineering (ICSE 03)*, Portland, OR, 705-715.

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

Knight, M. B., & Pearson, J. M. (2005). The changing demographics: The diminishing role of age and gender in computer usage. *Journal of Organizational and End User Computing, 17*(4), 49-65.

Kostakos, V., & O'Neill, E. (2008). Human in the loop: Rethinking security in mobile and pervasive systems. *ACM Proceedings of the 26th Annual SIGCHI Conference on Human Factors in Computing Systems 2008,* Florence, Italy, 3075-3080.

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

Kshetri, N. (2006). The simple economics of cybercrimes. *IEEE Security & Privacy, 4*(1), 33-39.

Kumaraguru, P., Rhee, Y., Acquisti, A., Cranor, L., Hong, J., & Nunge, E. (2007). Protecting people from phishing: the design and evaluation of an embedded training e-mail system. *ACM Proceedings of the SIGCHI Conference on Human Factors in Computing Systems 2007,* San Jose, CA, 905-914.

Lampson, B. W. (2004). Computer security in the real world. *IEEE Computer, 37*(6), 37-46.

Levy, E. (2004). Criminals become tech savvy. *IEEE Security & Privacy, 2*(2), 65-68.

Lipinski, S., Cooper, M., Cook, C., & Orndorff, C. (2007). iS3PACE – casting the information security spell for cultural change. *ACM Proceedings of the 35th Annual ACM SIGUCCS Conference on User Services*, Orlando, FL, 41-45.

Locke, L., Spirduso, W., & Silverman, S. (2000). *Proposals that work: A guide for planning dissertations and grant proposals* (4th ed.). Thousand Oaks, CA: Sage.

MacInnes, I., Musgrave, D., & Laska, J. (2005). Electronic commerce fraud: Towards an understanding of the phenomenon. *IEEE Proceedings of the 38th Hawaii International Conferences on System Sciences 2005 (HICSS 05),* Big Island, HI, 1-11.

McDowell, K. (2006). Now that we are all so well-educated about spyware, can we put the bad guys out of business? *ACM Proceedings of the 34th Annual Special Interest Group on University & College Computing Services 2006 (SIGUCCS 06),* Edmonton, Alberta, Canada, 235-239.

Mitnick, K., & Simon, W. (2002). *The art of deception*. Indianapolis, IN: Wiley.

Moncur, W., & Leplatre, G. (2007). Pictures at the ATM: Exploring the usability of multiple graphical passwords. *ACM Proceedings of the SIGCHI Conference on Human Factors in Computing Systems 2007,* San Jose, CA, 887-894.

Moore, C. (2004). The growing trend of government involvement in IT security. *ACM Proceedings of the 2004 Conference on Information Security Curriculum Development (InfoSecCD 04),* Kennesaw, GA, 119-123.

Nardi, P. (2003). *Doing survey research: A guide to quantitative methods*. Boston, MA: Pearson.

North, M. M., George, R., & North, S. M. (2006). Computer security and ethics awareness in university environments: A challenge for management of information systems. *ACM Proceedings of the 44th Annual Southeast Regional Conference (ACM SE-44),* Melbourne, FL, 434-439.

North, M. M., George, R., & North, S. M. (2007). A brief study of information security and ethics awareness as an imperative component of management information systems. *ACM Proceedings of the 45th Annual Southeast Regional Conference (ACM SE-45),* Winston-Salem, NC, 515-516.

Ohaya, C. (2006). Managing phishing threats in an organization. *ACM Proceedings of the 3rd Annual Conference on Information Security Curriculum Development 2006 (InfoSecCD 06),* Kennesaw, GA, 159-161.

Orgill, G. L., Romney, G. W., Bailey, M. G., & Orgill, P. M. (2004). The urgency for effective user privacy education to counter social engineering attacks on secure computer systems. *ACM Proceedings of the 5th Conference on Information Technology Education,* Salt Lake City, UT, 177-181.

Paulson, L. D. (2002). Post 9-11 security: Few changes, business as usual rules. *IEEE IT Professional, 4*(4), 10-13.

Raghavan, V. V., Sakaguchi, T., & Mahaney, R. C. (2008). An empirical investigation of stress factors in information technology professionals. *Information Resources Management Journal, 21*(2), 38-62.

Ramim, M., & Levy, Y. (2006). Securing e-learning systems: A case of insider cyber attacks and novice IT management in a small university. *Journal of Cases on Information Technology, 8*(4), 24-34.

Reeder, R. W., & Arshad, F. (2005). SOUPS 2005. *IEEE Security & Privacy, 3*(5), 47-50.

Sankarapandian, K., Little, T., & Edwards, W. K. (2008). Talc: Using desktop graffiti to fight software vulnerability. *ACM Proceedings of the 26th Annual SIGCHI Conference on Human Factors in Computing Systems 2008,* Florence, Italy, 1055-1064.

Sasamoto, H., Christin, N., & Hayashi, E. (2008). Undercover: authentication usable in front of prying eyes. *ACM Proceedings of the 26th Annual SIGCHI Conference on Human Factors in Computing Systems 2008*, Florence, Italy, 183-192.

Shneiderman, B., & Plaisant, C. (2005). *Designing the user interface* (4th ed.). New York, NY: Addison Wesley.

Singh, S., Cabraal, A., Demosthenous, C., Astbrink, G., & Furlong, M. (2007). Password sharing: Implications for security design based on social practice. *ACM Proceedings of the SIGCHI Conference on Human Factors in Computing Systems 2007*, San Jose, CA, 895-904.

Siponen, M. T., & Oinas-Kukkonen, H. (2007). A review of information security issues and respective research contributions. *ACM SIGMIS Database, 38*(1), 60-80.

Smith, S. W. (2003). Humans in the loop: Human-computer interaction and security. *IEEE Security & Privacy, 1*(3), 75-79.

Spitzner, L. (2003). Honeypots: Catching the insider threat. *IEEE Proceedings of the 19th Annual Computer Security Applications Conference (ACSAC 2003)*, Las Vegas, NV, 170-179.

Stahl, B. C. (2004). Responsibility for information assurance and privacy: A problem of individual ethics. *Journal of Organizational and End User Computing, 16*(3), 59-77.

Stefanek, G. (2002). *Information security best practices: 205 basic rules*. Woburn, MA: Butterworth-Heinemann.

Stoll, J., Tashman, C. S., Edwards, W. K., & Spafford, K. (2008). Sesame: Information user security decisions with system visualization. *ACM Proceedings of the 26th Annual SIGCHI Conference on Human Factors in Computing Systems 2008*, Florence, Italy, 1045-1054.

Suchan, W. K. (2003). A model-based approach to achieve organizational information assurance. *Dissertation Abstracts International, B 64*(06), 2761. (UMI No. 3095004).

Toomim, M., Zhang, X., Fogarty, J., & Landay, J. (2008). Access control by testing for shared knowledge. *ACM Proceedings of the 26th Annual SIGCHI Conference on Human Factors in Computing Systems 2008*, Florence, Italy, 193-196.

Tsai, J. Y., & Egelman, S. (2006). SOUPS 2006. *IEEE Security & Privacy, 4*(6), 53-55.

Tucker, T. (2002). 2002 security awareness index report: The state of security awareness among organizations worldwide. *PentaSafe*. Retrieved April 27, 2008, from http://www.pentasafe.com

Twitchell, D. P. (2006). Social engineering in information assurance curricula. *ACM Proceedings of the 3rd Annual Conference on Information Security Curriculum Development 2006 (InfoSecCD 06)*, Kennesaw, GA, 191-193.

Van Dyke, T. P. (2007). Ignorance is bliss: The effect of increased knowledge on privacy concerns and Internet shopping site personalization preferences. *International Journal of Information Security and Privacy, 1*(2), 74-92.

Vatsa, V., Sural, S., & Majumdar, A. (2007). A rule-based and game-theoretic approach to online credit card fraud detection. *International Journal of Information Security and Privacy, 1*(3), 26-46.

Waikar, A., & Huynh, M. Q. (2008). How can Internet service providers tap into the potentially-lucrative small business market? *International Journal of E-Business Research, 4*(1), 82-98.

West, R. (2008). The psychology of security. *Communications of the ACM, 51*(4), 34-40.

Whitman, M., & Mattord, H. (2003). *Principles of information security*. Boston, MA: Thomson Course Technology.

Wu, M., Miller, R. C., & Garfinkel, S. L. (2006). Do security toolbars actually prevent phishing attacks? *ACM Proceedings of the Annual SIGCHI Conference on Human Factors in Computing Systems 2006*, Montreal, Quebec, Canada, 601-610.

Zukowski, T., & Brown, I. (2007). Examining the influence of demographic factors on Internet user's information privacy concerns. *ACM Proceedings of the 2007 Annual Research Conference of the South African Institute of Computer Scientists and Information Technologists on IT Research and Developing Countries*, Elizabeth, South Africa, 197-204.