

2015

An Exploration of Wireless Networking and the Management of Associated Security Risk

Helen Loretta Collins
Walden University

Follow this and additional works at: <https://scholarworks.waldenu.edu/dissertations>

 Part of the [Business Administration, Management, and Operations Commons](#), [Databases and Information Systems Commons](#), [Management Sciences and Quantitative Methods Commons](#), and the [Other Communication Commons](#)

This Dissertation is brought to you for free and open access by the Walden Dissertations and Doctoral Studies Collection at ScholarWorks. It has been accepted for inclusion in Walden Dissertations and Doctoral Studies by an authorized administrator of ScholarWorks. For more information, please contact ScholarWorks@waldenu.edu.

Walden University

College of Management and Technology

This is to certify that the doctoral dissertation by

Helen Loretta Collins

has been found to be complete and satisfactory in all respects,
and that any and all revisions required by
the review committee have been made.

Review Committee

Dr. Nikunja Swain, Committee Chairperson, Management Faculty

Dr. Anthony Lolas, Committee Member, Management Faculty

Dr. Judith Forbes, University Reviewer, Management Faculty

Chief Academic Officer

Eric Riedel, Ph.D.

Walden University

2015

Abstract

An Exploration of Wireless Networking and the Management of
Associated Security Risks

by

Helen Loretta Collins

BS, Information Systems, Strayer University, 1996

MS, Administration, Central Michigan University, 2000

MS, Software Engineering Administration, Central Michigan University, 2000

Dissertation Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Philosophy

Applied Decision Sciences

Walden University

February 2016

Abstract

The rapid expansion of wireless information technology (IT) coupled with a dramatic increase in security breaches forces organizations to develop comprehensive strategies for managing security risks. The problem addressed was the identification of security risk management practices and human errors of IT administrators, putting the organization at risk for external security intrusion. The purpose of this non-experimental quantitative study was to investigate and determine the security risk assessment practices used by IT administrators to protect the confidentiality and integrity of the organization's information. The research questions focused on whether the security risk management practices of IT administrators met or exceeded the minimally accepted practices and standards for wireless networking. The security risk assessment and management model established the theoretical framework. The sample was 114 participants from small to medium IT organizations comprised of security engineers, managers, and end users. Data collection was via an online survey. Data analysis included both descriptive and inferential statistical methods. The results revealed that greater than 80% of participants conducted appropriate risk management and review assessments. This study underscored the need for a more comprehensive approach to managing IT security risks. IT managers can use the outcome of this study as a benchmark for evaluating their current risk assessment procedures. Experiencing security breaches in organizations may be inevitable. However, when organizations and industry leaders can greatly reduce the cost of a data breach by developing effective risk management plans that lead to better security outcomes, positive social change can be realized.

An Exploration of Wireless Networking and the Management of
Associated Security Risks

by

Helen Loretta Collins

BS, Information Systems, Strayer University, 1996

MS, Administration, Central Michigan University, 2000

MS, Software Engineering Administration, Central Michigan University, 2000

Dissertation Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Philosophy

Applied Management and Decision Sciences Program

Walden University

February 2016

Dedication

This research paper is in loving memory of my great-great grandmother

Mrs. Rebecca Fernandez.

Acknowledgments

I would like to thank my son Ray Anthony Collins Jr. for sharing this journey with me, for buying my books, paying for tutors, paying the rent, and keeping the lights on so I could study. I acknowledge the Defense Health Agency (DHA) Component Acquisition Executive, Mr. Michael O'Bar and Deputy Component Acquisition Executive Robert Bolluyt for believing in me and providing me the infrastructure and tuition assistance I needed to develop a new career. A special thanks to my colleagues at the DHA who were my sounding boards. To the lifelong friends I have made, Frederick, Mo, and Chuck, thanks for the extensive conversations, sharing of lessons learned, and for becoming intellectual partners as we collaborated and worked our way through our research projects. To Dr. Louis Taylor who helped me stay on track when I lost my direction, thank you! To my Committee Chairs Dr. Nikunja Swain and Dr. Anthony Lolas, I cannot thank you enough for your patience, your willingness to take the time to explain concepts such as anthropomorphism, for your reassurance, and teaching me the importance of critical thinking in research and writing. Last but not least, I thank GOD for giving me the strength to go the distance, for taking me from sick, homeless, unemployed, to a new homeowner and a new career.

Table of Contents

List of Tables	iv
List of Figures	v
Chapter 1: Introduction to the Study.....	1
Introduction.....	1
Background of the Study	4
Problem Statement.....	7
Purpose of the Study	9
Research Questions and Hypotheses	10
Theoretical Foundation.....	13
Nature of the Study.....	14
Definitions	15
Assumptions, Limitations and Scope.....	16
Assumptions.....	16
Limitations	16
Scope.....	17
Significance of the Study	17
Significance to Theory	17
Significance to Practice.....	18
Significance to Social Change	19
Summary.....	20
Chapter 2: Literature Review	21
Introduction.....	21

Literature Search Strategy	21
Theoretical Foundation	22
Additional Theoretical Perspective and Wireless Security Models.....	25
Wireless Learning Theoretical Framework	33
Literature Review	34
Wireless Security Threats and Issues.....	38
Security and Information Security	40
Information Systems Security Risk Management.....	40
Users	44
Federal Trade Commission (FTC) Standards and Enforcement.....	47
Security Risk Assessment (SRA) Model	48
Other Studies and Methodologies on Wireless Securities	49
Summary and Conclusions	55
Steps in Performing Risk Analysis	56
Chapter 3: Research Method.....	61
Introduction.....	61
Research Design and Rationale	61
Methodology	64
Population and Sampling	64
Recruiting Procedures	65
Instrumentation	65
Operationalization.....	66
Data Analysis Plan	68

Threats to Validity	71
Ethical Procedures	72
Summary	74
Chapter 4: Results	76
Introduction.....	76
Data Collection	77
Data Analysis	78
Study Results	83
Summary.....	86
Chapter 5: Summary, Conclusion, and Recommendations	88
Introduction.....	88
Interpretation of Findings	88
Limitations of the Study	97
Recommendations.....	98
Implications	101
Conclusions.....	106
References.....	107
Appendix A: Wireless Questions from Security Self-Assessment Tool	124
Appendix B: Descriptive Statistics	125

List of Tables

Table 1 Types of Wireless Connectivity..... 35

Table 2 Categories of Users 46

Table 3 Secure Aware Routing Properties and Techniques..... 53

Table 4 Research Questions/, Survey Questions, and Analysis..... 73

Table 5 Reliability Statistics 79

Table 6 Industry Type..... 79

Table 7 Frequency Summary for All Categories 80

Table 8 Chi-Square Test Statistics 82

Table 1 One Sample83

Table 10 Risk Management 84

Table 11 Data Integrity and Protection..... 85

List of Figures

Figure 1. Technology acceptance model	34
Figure 2. Security as a process (Phifer, 2008).	56

Chapter 1: Introduction to the Study

Introduction

The topic of this study focused on the exploration of wireless networking and the management of associated security risks. Network and computer security threat incidents are on the rise, and both corporations and governments are continuing to investigate ways to effectively manage the challenges those threats create (Sabnis, Verbruggen, Hickey, & McBride, 2012). The rapid growth of wireless networking for personal and business use has forced the division of wireless applications into different standards directions. Many common standards such as Zigbee (IEEE 802.15.4-2006) and Wi-Fi (IEEE 802.11) are being used in wireless networks (Maheshwari & Kemp, 2012). With the development of new wireless technologies and new devices with more features and ease of use come new security risks.

The reality of security breaches is not limited to large, public organizations. Careless and reckless employees present serious threats to their organizations when they fail to follow information security policies (Siponen, Mahmood, & Pahlila, 2009). Sabnis et al. (2012) reported that in 2010, approximately three billion cyber-attacks on companies and government agencies, costing large organizations an average of 7.2 million dollars, with the greatest conveyed expenditures exceeding \$35 million for security breaches (successful attacks). Large organizations are targeted because, in many cases, they do not protect their large databases with the best technology available (Shiple, 2010). In 2014, the University of Maryland detected a cyber-attack to a database that held records and social security numbers for students, alumni, faculty, and

others associated with the school over a 20-year period (Dance, 2014). The Chief Information Officer (CIO) was among the 287,000 victims (Dance, 2014).

The Department of Veterans Affairs had their eBenefits website malfunction, which allowed customers to log into the accounts of others without the account holders' permission (Veteran's, 2014). The website was supposed to make transactions easier for veterans; however, because of the breach, the website was shut down, the old system was re-instated, until the glitches were fixed within a few days and the newly established system fully operational (American Legion, 2014).

In South Carolina, the Department of Revenue experienced two attempts by hackers, in August and September of 2012, to crack into state-protected personal information (Zolkos, 2012). It was then revealed in October 2012 that hackers breached the Department of Revenue's database and collected in excess of 3.5 million social security numbers and an additional 387,000 credit and debit cards (Zolkos, 2012). On September 1, 2013, the South Carolina State newspaper reported that the cost to the state equaled \$21,660,022, whereas a \$25,000 dual logon system would have prevented the breach. Since the initial breach, the South Carolina Department of Revenue took several measures to secure the system and contracted with an Information Systems (IS) company to assist with investigation of the breach. New equipment and software were installed and controls on access to the system were tightened. The system is believed to be more secure now (Zolkos, 2012).

Target, a large major retailer, had its database breached in late 2013 and over 40 million customers had their personal information, including financial information, stolen

(Crosman, 2014). Almost all established enterprises are targets, and the attacks have become more sophisticated as evidenced by the emergence of advanced persistent threats. However, public organizations are not the only ones that have security breaches.

A security breach that had the potential to affect 70 million people occurred with Sony in 2011 (Yen, 2011). Sony's PlayStation Network was the victim of hackers accessing personal data for approximately 70 million Sony's PlayStation Network members. The information that was taken, in many cases, included addresses, credit card information, passwords, logins, and even security answers for the passwords (Yen, 2011). This fraudulent access can cause personal devastation for years.

The aforementioned incidents clearly indicated a need for this study. The situations presented provided evidence that any person or organization can be affected by such an attack. Positive social change will be realized when Information Technology (IT) professionals can find ways to ensure that critical assets remain protected. That means implementing security measures that allow using wireless networks free of attacks on the system.

Chapter 1 presents a detailed overview of this study beginning with an introduction to the background of the study followed by a statement of the problem. Other major headings included in this chapter are Purpose of the Study, the Nature of the Study, Research Questions, Definitions, Assumptions, Limitations and Scope, Significance of the Study, and Summary.

Background of the Study

Security breaches have overwhelming effects on an organization's mission and goals, leaving organizations puzzled with how to proceed next. Obviously, Information System Administrators want to prevent security breaches to minimize rising costs. Too often, cost/benefit analysis has an impact on the magnitude of prevention efforts. Organizations want to manage their risks sensibly, but because many lack knowledge of the important parameters, they cannot make good decisions or explain their policies to users (Lampson, 2009). To address these challenges, a need is present to assess and determine how organizations successfully manage security risks to make systems trustworthy.

Information security has become an essential resource for corporations to conduct business operations and to communicate with their clients and investors (Ayyagari, 2012). Consequently, the burden is on corporations to preserve the confidentiality, integrity, and availability of these systems to operate and to sustain the confidence of stakeholders. Not surprisingly, this kind of reliance on Automated Information System (AIS) has also seen an increased in the number of attacks and security breaches (Privacy Rights Clearinghouse, 2011). Therefore, issues related to information security and privacy have become one of the core apprehensions of corporations and information technology (IT) managers (Information Systems Audit and Control Association, 2009-2014).

Alshboul (2010) reported that security-related losses cost the U.S. economy an estimated at \$117.5 billion a year, causing devastating aftereffects on both the

marketplace and nationwide safety. Additionally, a security breach could cost an organization to lose personal information, resulting in a breach of confidentiality and integrity. The security of data is the main requirement of any IT organization (Kaur, Rana, & Rishma, 2012). In this technological era, data are sent and received in many electronic forms, often exposing companies to increased data hacks, threats, and losses. Many employees in IT organizations handle sensitive personal identification data on a daily basis; therefore, having secure network connections is of the utmost importance.

In many IT organizations, wireless communication is one of the most rapidly developing telecommunications technologies that allows users to integrate their personal network with a global network and access a wide range of services (Kim, 2013). To access the Internet today, many laptops or other mobile computer devices are equipped with multiple heterogeneous wireless network interfaces (Kassar, Kervella, & Pujolle, 2008). Wireless networking provides many advantages, but poses new security threats and alters the organization's overall information security risk profile. Unlike wired networks, where data are stored in cables, a wireless network uses open air as a broadcast medium. This form of wireless networking introduces a greater risk from would-be intruders (Dhull & Singh, 2010; Likhar, Yadav, & Rao, 2011).

Although implementation of technological solutions is the normal response to wireless security breaches and threats, wireless security remains an organizational management issue (Kirankumar, Babu, Prasad, & Vishnumurthy, 2012). Many users may know that wireless communications are susceptible to security risks. However, the

reasons for these risks and how network managers manage security risks are not well understood by users of the networks (Berghel & Uecker, 2005).

Wireless networking presents many advantages. These advantages include improved productivity due to increased accessibility to information resources (Kirankumar et al., 2012). The second most notable advantage is network configuration and reconfigurations are simpler, quicker, and less costly. Nevertheless, along with the advantages of wireless technology, associated vulnerabilities are present. Wireless networks can alter the existing information security risk, which results in a host of risk issues for information systems (IS) managers. IS managers can face unauthorized access points, broadcasted Service Set Identifier (SSIDs), and spoofed Media Access Control (MAC), just a few of the problems Wireless Local Area Networks (WLAN) present (Kirankumar et al., 2012). Wireless networks are more susceptible to security risks than wired networks due to the mode of data dissemination. Wireless sensor network nodes are placed in unprotected, hostile, or dangerous environments using radio frequencies. The risk of interception becomes greater than with wired networks (Kirankumar et al., 2012).

Internet services offer many advantages to business organizations, including worldwide trade, cost reduction, and increased productivity (Bojanc & Jerman-Blazic, 2013). Any unwanted Internet invasion or unforeseeable attack on IS will result in substantial losses and stalled business operations. These security risks may occur in several ways, most notably from human errors, fraud, or external intrusions. For these reasons, more businesses invest in technologies for protection of the company's

information assets. Although modern security technologies have greatly improved in ways to protect the assets, confidentiality, and integrity of businesses, more innovations and interventions are needed to improve the security levels of computers and networks (Bojanc & Jerman-Blazic, 2013).

All organizations that have AIS, Websites, intranet, and Internet are subject to an increased number of security threats (Alshboul, 2010). Garfinkel (2012) claimed that the penetrations and data thefts of the most sensitive systems occur weekly. This means that modern computer systems are actually less secure than systems were a decade ago and the problem is getting worse (Garfinkel, 2012). This study was needed to address gaps in the literature and in key technical aspects of information security, and to deliver possible security solutions. It is important to raise organizational awareness of security risks and the development and performance of security controls (Spears & Barki, 2010).

Problem Statement

The problem this study addressed was the lack of effective security practices required for managers and IT administrators to protect and manage the security threats associated with wireless networking in the organization. The aim was to investigate the security measures managers take to protect the availability, confidentiality, and integrity of the IT organizations, both to ensure more reliable communication and to increase security (Vanitha, Selvakumar, & Subha, 2013). The cost of recovery from a security breach is many times greater than the cost of prevention (Jones, McCarthy, & Halawi, 2010). Furthermore, Jones et al. (2010) reported that when a data breach occurs, companies with volumes of customer accounts can spend upwards of \$90 per customer

for recovery compared to a range between \$6 and \$16 per customer on data encryption, intrusion detection, and prevention.

The risks associated with wireless technology are considerable, despite numerous benefits such as employee mobility, convenience, and ease of use. This risk is especially true when wireless technology can transmit confidential or sensitive information. Thus, maintaining a secure wireless network requires greater effort than traditional wired networks. Yet, the overall security objectives for IS managers of wireless networks remain the same as for wired networks: (a) preserving confidentiality, (b) ensuring integrity, and (c) maintaining availability of the information (Bojanc & Jerman-Blazic, 2013). With the rapid growth of wireless networking in IT organizations, more research is needed on specific techniques and measures to identify and manage the security threats uniquely associated with wireless networking.

Every company fears a stoppage of business and interruption of the flow of vital information due to security breaches, among other problems, which prevent employees from performing vital work functions (Bojanc & Jerman-Blazic, 2013). Such security breakdowns interrupt the processing of information to consumers and vendors on a real-time basis (Vanitha et al., 2013). Chickowski (2013) claimed that IT is fraught with vulnerabilities, which is a growing problem that organizational leaders must come to understand. Security risks in the transmission of sensitive information are exacerbated by continual technological innovation. In response, more and more organizations are devising risk management plans to handle situations involving incidents of hacking, copyright infringement, and defamation (Chickowski, 2013). It is crucial that

organizations employ effective methods for conducting IT risk assessment. The frequency with which they conduct the risk assessment process is almost as important as the means by which they do so. Although organizations may be thorough in performance of routine IT risk assessments, such efforts should be repeated often enough to keep abreast of new risks (Chickowski, 2013).

In summary, IT managers should understand that threats of information breaches are real, and they should be willing to exercise appropriate measures to ensure that information security strategies, policies, and procedures are communicated and enforced. Destruction or loss of information or AIS could seriously affect the bottom-line of the organization as well as the company's reputation.

Purpose of the Study

The purpose of this nonexperimental quantitative study was to investigate and determine the security risk assessment practices IT administrators use to protect the confidentiality and integrity of each organization's information. The aim was to assess how IT managers of these organizations identify security threats associated with wireless networking. Security is one of the major concerns with wireless networks because a typical wireless network is easy to access (Kirankumar et al., 2012). Software is available that can intercept radio signals traveling through the atmosphere. Individuals near the vicinity of the organization with the right software can easily intercept the signals. To prevent security breaches, management needs to identify the vulnerabilities that exist within the organization and decide how to eliminate or minimize them (Taylor & Brice, 2012). Practicing IT/IS managers should be able to control security risks to develop

systems and services that satisfy clients' requirements (Bojanc & Jerman-Blazic, 2013). Many users today utilize weak security techniques, and their wireless networks can easily be attacked for unauthorized access. For example, a security feature such as Wired Equivalent Privacy (WEP) could easily be attacked with the ample availability of tools (Vanitha et al., 2013).

Xu, Hu, and Zhang (2013) maintained that organizations should perform security assessments before implementing wireless technologies to determine the specific threats and vulnerabilities of wireless networks in organizational environments. Consideration of existing security policies, potential threats and vulnerabilities, company policies, safety issues, and costs for security measures are necessary (Borrett, Carter, & Wespi, 2013; Spears & Barki, 2010). When the risk assessment is complete, the organization can begin planning and implementing the measures necessary to safeguard their systems and reduce their security risks to a manageable level. The policies and measures put in place should periodically be re-assessed because technologies and malicious threats are constantly changing.

Research Questions and Hypotheses

The research questions of this study were designed to investigate and assess the security practices by which IT administrators handle the security threats associated with wireless networking in the IT organization. They are the following:

RQ1: What security risk assessments, if any, do IT administrators perform to protect the confidentiality and integrity of the organization's information?

H_01 : IT administrators do not regularly perform security risk assessments to protect the confidentiality and integrity of the organization's information.

H_a1 : IT administrators regularly perform security risk assessments to protect the confidentiality and integrity of the organization's information.

Central to this study is network security risk management practices of IT administrators, which involve mainly wireless networking. However, network security includes the entire system of transport and storage technologies system, which is comprised of computers, routers, cables, switches, and wireless access points (Ansilla, Vasudevan, & Ravi, 2015). Research question one was designed to obtain information in general about the security risk management practices of the organization. It is important to conduct risk assessment regularly in order to identify and prioritize vulnerabilities for remediation. The frequency to which risk assessment should be performed depends on numerous factors, such as magnitude of the network and number of workforce personnel (SECNAP, 2012). After the initial risk assessment, most companies select a mixture of monthly external analyses and quarterly internal analyses. Extremely, large corporations commonly choose to perform both internal and external analyses on a monthly basis.

RQ2: Do network security risk management practices of IT administrators meet the minimally accepted practices and technical standards for wireless networking as measured by a security self-assessment survey?

H_02 : The network security risk management practices of IT administrators do not meet the minimally accepted practices and technical standards for wireless networking as measured by a security self-assessment survey.

H_{a2} : The network security risk management practices of IT administrators do meet the minimally accepted practices and technical standards for wireless networking as measured by security self-assessment survey.

Researchers believe significant security risks are associated with handling of personal information using wireless networks. Therefore, it is important that IT managers carefully explore and consider how they use wireless technology to handle personal information and ensure that their wireless technology is as secure as possible. IT administrators may already be aware of the proper techniques for securing the wired medium itself, yet it is unclear whether IT administrators perform security risk assessments that follow generally accepted practices and meet technical standards. Chickowski (2013) argued that while it may be essential that security organizations employ effective IT risk assessments, it is imperative that acceptable standards are achieved during implementation. When IT administrators fail to adhere to generally accepted practices and technical standards, they could be exposing their systems to significant security risk. With new developments in wireless communications networks and with the ubiquitous use of wireless user devices, new security risks arise that IT managers of organizations must address (Kim, 2013).

Steps should be taken to ensure that critical assets remain protected. Therefore, it is important to examine the management of security issues of wireless and wired networks for information processing in the corporate or organizational environment. Many security problems can be traced back to the end user in wired networks. As network perimeters expand, IT administrators should find solutions that provide defenses

that are appropriate and manageable for wired and wireless organizational environments (Thangavel & Thangaraj, 2011).

Theoretical Foundation

The theoretical foundation for this study was the risk management theory proposed by Kwo-Shing Hong, Yen-Ping, Chao, and Tang (2003). The key tenet of this risk management theory is that threats and vulnerabilities could be evaluated and assessed through organizational risk analysis and assessment. The results from the assessments could be used for designing data security prerequisites and risk control instruments. The primary aim is to minimize security risk to a target level in a business. The considerable usage of wireless transmission mechanisms and the increasing interconnectivity among systems expose businesses to major security risk and vulnerabilities, including premeditated threat. Therefore, interest is growing in applying risk analysis and risk management to identify and reduce security issues and protect systems (Kwo-Shing Hong et al., 2003).

A risk assessment framework is needed with an approach for categorizing and sharing information about the security risks of the IT infrastructure (Saleh, Refai, & Mashhour, 2011). Saleh et al. (2011) defined security risk assessment as a model for evaluating security risks. They conducted the assessment at the first stages of the system development and as changes to data or its infrastructure occurred. The process was important to identify threats and vulnerabilities that could penetrate the IT infrastructures.

The primary objective of risk management is to avoid not only business losses, but also to provide a way to recognize opportunities that can benefit the society and

businesses. Because it is impossible to identify all risks in the early stages, risk assessment should be reviewed continuously. The framework established provisions for design, collection, analysis, and reporting of survey data in this study. An in-depth discussion is presented in the Chapter 2 literature review.

Maintaining secure wireless networks takes more frequent risk assessment and control evaluation than is required for other systems and networks (Radack, 2013). Several steps can be taken by IT managers to achieve quality management of wireless systems. They should (a) fully understand wireless network topology, (b) conduct frequent inventory on handheld and wireless devices, and (c) back up data continually. Additionally, they should (d) periodically test and assess wireless network security, and (e) track for standard changes in the wireless industry that would not only improve security, but also allow the release of new merchandise (Radack, 2013).

Nature of the Study

The research design selected for this non-experimental quantitative study was a self-reported, web-based survey using a cross-representation of industries and company sizes. SurveyMonkey was selected as the online survey vendor. The targeted population was experienced IS managers, security engineers, and other individuals responsible for designing, implementing, securing, using, and maintaining wireless networking security. They were positioned to provide reliable assessments of the study variables at both the organizational and consumer levels. Data analysis included both descriptive and inferential statistics. A detailed description of the research design, methodology, and sampling procedures are presented in Chapter 3 of the methodology component.

Definitions

The following is a list of definitions and interpretations of key variables and terms that are used throughout the dissertation.

Automated information system (AIS): AIS is a system that performs functions such as collecting, processing, storing, transmitting and displaying information (Defense Acquisition University, 2014).

Information security: The set of practices, policies, personnel, and technology charged with safeguarding a business's data assets (Alshboul, 2010).

Information technology (IT): IT is any equipment such as computers, ancillary equipment, or software used in the storage, manipulation, management, movement, control, display, transmission, or reception of data or information by the executive agency (Defense Acquisition University, 2014).

Information technology organization: Information technology organization is an organization with a division within the company that oversees the establishing, monitoring, and maintaining of information technology systems and services by ensuring no concerns were present about the compromise of data when distributed (Pazos, Chung, & Micari, 2013).

IT organization: IT organization is any organization that is a consumer of computer services utilizing wired or wireless services. IT organization members include managers, administrators, engineers, and end users.

Security risk management (SRM): SRM refers to established plans and processes for assessing network security risks (Bojanc, & Jerman-Blazic, 2013).

Security measures: Security measures are actions taken to prevent or minimize the damage caused by the invasion of single or multiple threats (Bojanc, & Jerman-Blazic, 2013).

Security threat: A security threat is a state of vulnerability where information security might be compromised (Kumar, Park, & Subramaniam, 2008).

System vulnerabilities: *System vulnerabilities are* weaknesses that reduce a system's ability, data integrity, and confidentiality (Bojanc & Jerman-Blazic, 2013).

Assumptions, Limitations and Scope

Assumptions

As in all research, assumptions and limitations exist. In the present study, the following underlying assumptions were:

1. The participants' responses to survey questions would reflect honesty and thoughtfulness.
2. The sample was representative of the population of IT organization members, which included managers, administrators, engineers, and end users.
3. Anonymity and confidentiality were preserved and that the participants were volunteers who would withdraw from the study at any time and with no ramifications.

Limitations

Geographically, the survey was conducted within IT industries within the Northeastern region of the United States. As a result, findings may not generalize to other

organizations and businesses in regions throughout the United States. A key limitation was reliance on self-reported data, which might have been subject to recall biases inherent to questions being asked. A possibility was present that participants completing the Internet-based survey might have skipped questions or not completed the survey, resulting in self-reporting errors.

Scope

The scope of this study was limited to investigating the management of wireless security issues from the perspectives of IT managers or individuals responsible for designing, securing, using, and maintaining wireless networking security. The findings in this survey might not have reflected the thoughts of all IT managers.

Significance of the Study

Secure networks are needed within organizations to build trusting relationships with customers, suppliers, and other business partners. Creating trust relationships can improve the cash flow and profitability of the organization (Saleh et al., 2011). With increasingly high-speed networks, wired and wireless Internet services are targets for security threats.

Significance to Theory

All corporations need secure networks and should become more proactive in their security stances (Pandey, 2011). This study makes several contributions to theory and practice. It applies concepts from risk management literature for the purpose of looking for ways to effectively manage risk in the IT organization. From a theoretical perspective, the researcher needs to have visibility into the complete risk picture of the organization

and an understanding of how those risks interrelate in impacting the business. In an effort to effectively mitigate risk, I was able to assess and evaluate those risks through a risk management survey.

Significance to Practice

As businesses become more attractive to cybercriminals, risk management and data security and protection are increasingly important. Although the focus of this study was risk management assessment, which mainly addressed the technical aspects of risk such as data confidentiality and wireless security, it also addressed the need for risk management to encompass not just the technology risk aspects, but also organizational goals, objectives, and operating environment.

When the results of the study are disseminated in publications, it will afford industry experts intelligence on how employee acquiescence to security strategies can be adopted and managed successfully. As information security continues to be a major concern for corporations, studies of this nature can aid in the implementation of security strategies and recommendations as indicated in the survey. Understanding the management of risks and threats is essential for IT managers to make their corporations as secure as possible. The findings are available to be used as a significant part of an overall information security strategic plan. It could encourage IT managers to convince personnel that data security threats are real and these threats can produce irreversible damages to their business. The information gained will assure that IT employees are provided with adequate research-based evidence that can help prevent information security breaches.

Additionally, given the demand for a highly trained and qualified information security workforce, this study can offer useful insight to prospective IT security professionals, employers, and educational institutions. Specifically, this study's results should help companies and AIS security professionals understand and address the security issues pertaining to the increasing demands for wireless networking. By providing centralized control of wireless access and security policies and centralized management of the infrastructures, operational costs could decrease and best practices could increase the productivity of IT personnel (Kim, 2013).

Significance to Social Change

This study has many implications for positive social change in today's age of information technology. The spread of information networks in organizations has created a huge volume of information exchange between different networks, resulting in new security threats to national organizations (Roozbahani & Azad, 2015). Therefore, identification of these threats and ways of dealing with them is essential. The question raised in this regard is what are the needed strategies and policies to deal with security threats?

Both organizations and individuals can greatly benefit when security measures are properly addressed to protect the wireless networks and wireless devices used for business applications. When IT managers properly and frequently assess the risks associated with wireless technologies in their companies, they can effectively decrease the exposure to risk by taking early actions to communicate identifiable threats and vulnerabilities. These measures may include supervisory, operational, and technological

constraints. While this study may not avert all security infiltrations in an organization, it can be effective in bringing attention to how IT managers can reduce many of the common risks associated with wireless technology.

Summary

In Chapter 1, I presented an overview of the study of wireless networking and the management of associated security risks in IT organizations. The section headings include background information, the problem statement, the purpose statement, research questions and hypotheses, theoretical framework, nature of the study, and operational definitions. Researchers argued that network security is one of the basic elements of any AIS organization, creating the need for increased information security management (Bojanc & Jerman-Blazic, 2013). More organizations are required to implement comprehensive and logical forms of protection (Choi, Kim, Goo, & Whitmore, 2008). Weak security measures can lead to data breaches, which can cripple an organization from an economic and reputational standpoint (Rhodes & Kunis, 2011).

The focus of Chapter 2 is a review of peer-reviewed journals on the selected topic of this study. I reviewed a concise synopsis of the current literature that supported and established the relevance of the problem. The literature review includes an investigation of common security issues and challenges in wireless networking relevant to confidentiality, integrity, reliability, and authentication. In Chapter 3, I explain the methodology and research design of this study. The focus of Chapter 4 is a presentation of the results of the study followed by Chapter 5, conclusions and recommendations.

Chapter 2: Literature Review

Introduction

Both security and wireless communications in IT organizations are central to the focus of this study. The primary research question of this study queried the process of how AIS managers identify and manage the security threats associated with wireless networking in the IT organization as measured by the security risk assessment and management model. As conveyed in the problem statement, while IT administrators may already be aware of the proper techniques for securing the WLAN itself, it may be unclear what measures they should take to protect the organization from wireless threats. The term *wireless* refers to data transmitted from one point to another without the use of a physical medium, such as wires. Wireless technologies operate in the radio frequency (RF) spectrum between 3 Hz and 300 GHz (Wilkie & Mensch, 2012). The purpose of this non-experimental quantitative study was to examine the practices that IT administrators incorporate in their organizations to assess security risk toward protecting organizational integrity and confidentiality. The goal is to assess how well IT managers identify security threats that arise in an environment of wireless networking.

Literature Search Strategy

The literature review highlights key concepts of security of wireless networks; that is, how issues of wireless networks affecting corporations and residential setups should be addressed. Current studies and related methodologies are presented. The literature search strategy included a comprehensive search for primary resources in journals, books, and dissertation databases. Search terms and descriptors included:

wireless security, wireless threats, security network, wireless security, wireless networking, security level, vulnerability and risk analysis, Ad-hoc network, security, IEEE 802.11, attacks, and breaches to AIS security. The goal was to conduct separate searches using as many alternative words as possible.

In the literature section, the theoretical foundation based on risk assessment and analysis begins the discussion. I discussed wireless and wired networking and the risks associated with various threats to security. While wireless networks are exposed to many of the same risks as wired networks, they are vulnerable to additional risks as well. Therefore, the overall security objectives for wireless remains the same as with wired networks that preserve confidentiality (Manikandan, Parameshwaran, Hariharan, Kalaimani, & Sridhar, 2013). In the concluding section, I present my recommendations for future possible solutions to security issues.

Theoretical Foundation

The theoretical foundation for this study was based on a risk assessment and analysis framework. A risk assessment framework was needed for categorizing and sharing information about the security risks of the IT infrastructure (Saleh et al., 2011). The security risk assessment provided a view of existing security risk and the necessary safeguards needed for security management. A proper and efficient security risk assessment could result in improved outcomes (Saleh et al., 2011).

The term *risk* was used to describe the possible impact of threats to exposed and vulnerable information assets. Information assets were presented as values by using the

properties of confidentiality, integrity, availability and other properties essential to the organization. The value of information assets was described as the impact level of these properties (Spears & Barki, 2010). Edward Snowden, a former Central Intelligence Agency and National Security Agency (NSA) employee who had a top-level United States security clearance presented a major risk to valuable information when he took advantage of his access (Wall, 2013). It was reported that he stole hundreds of thousands of documents over a period of years from the NSA and revealed many of the documents to the rest of the world (Scherer & Shuster, 2013). He had access to millions of United States secrets without the concern that someone was supervising and watching what he did with the documents (Wall, 2013). The information that he possessed was so coveted by the rest the world that the Ecuadorian, Russian, and Venezuelan governments offered Snowden political asylum. He ended up accepting Russia's offer (Weisbrot, 2013). Interest in applying risk analysis and risk management is on the rise.

Tsai and Huang (2011) presented a wireless risk assessment method for managing wireless network security administratively. Both an assessment measure and a risk model were used. The former was an algorithm to determine "the risk value of the wireless network according to the risk model" (p. 801), while the latter monitored the wireless network risk modeling. In the model, Tsai and Huang took into consideration wireless attacks, system configurations, and security requirements. The four layers of this extended analytic hierarchy process were the following: risk, requirement, attack, and configuration. These distinct layers could help in addressing wireless network dynamics "because only the related layers are introduced to the assessment measure when changes

of the network are detected” (p. 801). The researchers’ assessment determines risk in relationships among attacks, configurations, and devices. Therefore, this assessment measure/risk model could competently predict risk as well as wireless network dependencies.

Bischoff, Sinay, and Vargová (2014) posited that risk management at an organizational level must be integrated with managerial processes and strategic planning, which includes, *inter alia*, having to review and monitor the processes of risk management. Bischoff et al. stated that to approach risk management comprehensively, an organization must interconnect security processes and safety generically.

In the present era of climate change, where disasters such as tornadoes can destroy entire towns in minutes, risk management is particularly important in the health management field that covers millions of patient medical records. Liao and Chueh (2012) posited that most of the negative information security events in health organizations are due to improper management.

Research Information Ltd. (2011b) summarized several steps from Recall, a leader on a worldwide scale in managing crucial business records in over 20 countries to have the following strategies set in the event of a disaster:

1. All critical documents as well as data backups should be stored off site, though if not available, then on-site infrastructure must be developed to protect against unauthorized users and natural events.

2. A Reliance Mobile Prepaid (RIM) plan must be created that contains lifecycle status of past and present documents communicated to employees so that critical business can keep functioning in all locations.
3. The functional and organizational areas like crucial departments, resources, vendors, and procedures, as well as other ways to obtain supplies that are critical to a secure document in emergencies must be identified.
4. Risk assessments must be performed for facility safety, physical document security, and who can access documents.
5. Annual document audits must be conducted as well as enactments of disaster retrieval.

Risk assessment and analysis was an appropriate choice for the theoretical framework of this study due to the significant rise in security breaches that organizations have to address, with the goal of determining how organizations can identify risks and address them to protect organizational integrity and confidentiality (Research Information Ltd., 2011b).

Additional Theoretical Perspective and Wireless Security Models

Yu and Weng (2013) discussed how hierarchical security can be introduced into wireless communication networks, demonstrating how information that is controlled and restricted flows through different security levels. I presented a two-tier hierarchical security model including intelligence data collection and command distribution. With communication of these two nodes, communication is effective if two additional models are fulfilled: Discretionary Access Control (DAC) and Mandatory Access Control

(MAC). The DAC offers the means for access control for the users themselves, and MAC uses mechanisms that are centralized to control access with formal policies. In order for messages to flow effectively from receivers and senders, wireless networks should fulfill both the DAC and MAC at the same time (Yu & Weng, 2013).

Yu and Weng (2013) noted that two conditions should be satisfied with a node that has the permission to send an e-mail. The first condition is if both the releaser and receiver nodes are located in the same cluster, and secondly, if the cluster being sent allows the e-mail to stream out and the receiver's cluster allows the e-mail to stream in. Every cluster head supports a portion of the entire distribution. The routing method described by Yu and Weng (2013) ensures that information confidentiality is not violated.

Friesen and McLeod's (2014) research on wireless security focused on the privacy with Wi-Fi connections in networks that may be unsecured, such as coffee shops. Places such as Ottawa Downtown area are described as having approximately 50% of the Wi-Fi unsecured. In such settings, people's card numbers and social network accounts such as Facebook and Twitter may be exposed to potential hackers. One respondent mentioned that just because it says it is free Wi-Fi, it does not mean it will not cost you later. Officials were aware of privacy issues, but specialists recommended that if there is private information to send, do not do it in public areas. Additionally, a recommendation was made that when sending information, especially when banks look for the HTTPS (Friesen & McLeod, 2014).

Wireless security ensures that a network is secure and provides the user with confidence that attackers cannot gain access to restricted areas. Security within networks continues to be a prevalent issue in all areas involving computing. Liu, Stimpson, Antonopoulos, Ding and Zhan (2014) examined the problems relating to the topic of wireless security and the background literature. Secretive information is continuously being transferred through Wi-Fi daily, such as emails and instant messaging (Liu et al., 2014). Many end users have little knowledge about computing. A recent example seen by many end users is the use of Wi-Fi on airplanes. Also, down loadable programs that are easily accessed by anyone compromise security on various networks at home or work.

Liu et al. (2014) indicated that poorly configured routers, with default passwords allow the attacker to connect or exploit weaknesses in the security system. A common trend Liu et al. found in an earlier study from 2006 to 2009 was the decreasing of older security types, which were identified as insecure. The results show that from 2006 to 2009 the drop in WEP usage was large and the slowing down from 2009 to 2012 may be attributed to the difficulty in ensuring that wireless security settings were changed by novice users. The overall findings indicated that encryption in wireless technology is improving.

Singh and Sharma (2014) discussed how protocols should be designed taking security issues and the most frequently observed attacks into consideration. His research identifies several frequently observed attacks associated with WSNs. Singh and Sharma illustrated how most attacks were caused by compromised nodes inserting false information. Attacks were divided into two categories, attacks against the security

mechanisms and attacks against the routing mechanisms. The most frequently observed attacks were denial of service (DoS), selective forwarding attack, sinkhole attack, and sybil attack.

Lalitha, Kumar, and Hamsaveni (2014) discussed a cluster-based technique for key management in wireless sensor network. The researchers noted that for supervising the physical world, the wireless sensor networks were the promising technology. Lalitha et al. reported that the threats and challenges of sensor networks are (a) spoofed, altered, or replayed routing information; (b) selective forwarding; (c) sinkhole attacks; (d) sybil attacks; (e) wormholes; (f) HELLO flood attacks; and (g) acknowledgement spoofing. The researchers categorize wireless channels into two possible security threats, inside threat and outside threat. A major difference between inside and outside threat was that the attacker does not possess control over the cryptographic material, whereas inside the attacker will possess some key materials and trust of some sensor nodes. Without tamper resistant hardware, compromising of the sensor nodes can be done easily.

Lalitha et al. (2014) viewed the proposed Energy Efficient Cluster Based Key Management (EECBKM) technique, which is evaluated through NS2 simulation. The EECBKM was compared to the SecLEACH scheme used by previous researchers. The performance was evaluated according to several metrics; average packet drop, average packet delivery ratio, and energy. The researchers found in the initial experiment that the numbers of attackers varied as 2, 4, 6, 8, and 10 from different clusters performing node capture attacks (Lalitha et al., 2014). The researchers noted that since the EECBKM decreases node capture attacks, the packet drop quantity resulted in less, when contrasted

with the present schemes. Whenever the quantity of attackers was increased, the packet drop followed resulting in an increase also (Lalitha et al., 2014).

Lalitha et al. (2014) noted that authentication in Wireless Sensor Networks (WSN) is a critical service for an unmanned system. The authentication is classified into: user authentication and authenticated querying. The user sends proof of his/her name of his identity to sensor node and user verification. WSN provides the authenticated query if the following properties are satisfied. First is safety, which is the query accepted by a sensor node only if the query was posted by an authorized user or derived from the WSN. Second is liveness: all sensors in WSN obtain legitimate query.

Data Integrity ensures data is not altered in transit by unauthorized parties
Data Freshness is defined as data that are current. A mechanism to monitor the age of messages is to include monotonically increasing counter with every message and reject messages with old counter values (Ramos & Holanda Filho, 2015). Data confidentiality is defined as keeping the data secure and unaltered by unauthorized parties. By encrypting the data with a secret key it will ensure only the correct receiver will only be able to receive the information. Symmetric key encryption methods are most highly used since public-key cryptography is expensive to use on complex sensor networks (Ramos & Holanda Filho, 2015).

Data authenticity prevents unauthorized parties from retrieving messages unintended for them. It can be attained through a sender and receiver sharing a secret key to compute a message authentication code (MAC) of all transmitted data. LEAP monitors whether nodes have been compromised since it shares a globally shared key for mass

messaging. Layered encryption and authentication mechanisms are essential to combatting security breaches. In today's society multiple users send data to multiple receivers over the same channel increasing the risk of security infrastructure. While this field is extremely broad, a huge concern is keeping networks completely security (Ramos & Holanda Filho, 2015).

Venkatraman et al. (2013) discussed various threats and challenges in keeping networks secure. A Denial of Service attack (DoS Attack) attempts to make a network unavailable for specific users. The attacker tampers with data prior to it being read by the sensor nodes by increasing the communication traffic (Venkatraman et al., 2013). This server overload results in inaccurate and slow readings. A Sybil Attack is when an attacker impersonates other nodes identities in the MAC. The attack can affect other protocol layers. An Eavesdropping attack is when the privacy of data is compromised. An attacker collects data such as the MAC address, cryptographic information user ID, password etc. The major concern with this attack is that the cryptographic information has been compromised which could lead to further data being accessed such as financial information (Venkatraman et al., 2013)

To increase the security of Wireless Body Area Networks (WBAN) Sivaprasatham and Venkateswaran (2012) proposed a key management technique to increases security. The WBAN is connected to the master server via the backend server using authentication channel. The information is relayed from the master server to the backend server. The nodes and master server will be able to transfer information by using a unique key. When a node wants to join a network, it sends the request message

protected by the MAC to the master server (Sivaprasatham & Venkateswaran, 2012). The master server verifies the MAC and generates a message key and a master key for the node. The message is encrypted by both servers and sends it to the node to initiate (Sivaprasatham & Venkateswaran, 2012).

Dong et al. (2012) discussed a security management system that has an effective and efficient scheme in wireless sensor networks. The researchers described a Wireless Sensor Network as consisting of a large number of micro, spatially distributed autonomous electronic devices using sensors to cooperatively monitor conditions both physical and environmental (Dong et al., 2012). The scheme was based on hierarchical structure of sensor networks. The simulation presented by the researchers demonstrated how the dynamic key management and behavior-based node abnormal detection method provide an entire security mechanism after the sensor nodes are deployed.

Dong et al. (2012) presented a diagram of topology of WSNs focusing on three entities: normal nodes, group heads, and sink nodes. Normal node has the capability of sensing and propagating the sensed data or receive the data and propagate to the next level node. The sink node is responsible for receiving, storing, and processing data from common nodes. Two layer structures are present, both lower and upper layers. The researcher's performance analysis was based on response time, detection rate, and false positive rate. The researchers concluded that the scheme presented provides a secure communication environment but also can detect the failure node or any suspicious nodes. Dong et al. (2012) found that the density and detection rate of the scheme increased, which was accompanied by the increase in the size of the WSNs. The number of sensor

nodes increased from 100 to 800, with the detection rate and false positive rate both having stable performance. The researchers found that scheme is flexible and adaptive to the network and expansion of the network (Dong et al., 2012).

Abiona et al. (2013) suggested the use of mobile agents to disperse dependable internet services delivery to clients. The proposed mobile agent approach guarantees secure authentication in wireless networks further examining the feasibility of the solution and wireless security model. The security in the wireless network environment is important since the transmission medium is pooled, which increases the difficulty in providing effective physical security controls in restricting ingress to the network.

The researchers proposed the mobile agent method to decipher the fundamental anomalies and security flaws in 802.1x authentication protocol (Abiona et al., 2013). The proposed security model involved three components supplicant, authenticator; and authentication server. The proposed mobile agent wireless authentication involves agent platforms, which are installed on both the authentication server and supplicant server. This allows Mobile Agents (MA) to run directly on them. Whenever a supplicant comes within range of an authenticator, a request is sent for identification of the supplicant. The supplicant later dispatches the Supplicant Mobile Agent (SMA) transmitting all data that is necessary for the supplicant (Abiona et al., 2013). The researchers noted that security is increased and re-authentication of client is completed in intervals during the connection. The process further ensures that a client cannot change their identity during a session.

Wireless Learning Theoretical Framework

Throughout the literature, it is evident that end users should be trained in the wireless technology and safety for security to be more effective. The technology acceptance model (TAM) outlined that perceived ease of use and perceived usefulness determine an individual's interaction to use a system with the intention to use serving as a mediator of the actual system use (Davis, 1989; Figure 1). The literature on security system focuses on the end user, and security management issues because of the lack of knowledge or implementation of the system (Friesen, 2014). The TAM proposed by Davis (1989) focused on the individual and intended use of a technological system. The model derives from the theory of reasoned action. TAM has behavioral elements, which outline that when a person forms an intention to act, the person will be free to act without limitation (Davis, 1989).

The theory of reasoned action originally proposed by Fishbein and Ajzen (1975) suggested that a person's actual behavior could be determined by considering his or her prior intention along with the beliefs that the person would have for the given behavior. Bandura (1982) demonstrated a similar theory, which complements areas of TAM, focusing on perceived usefulness and perceived ease. As demonstrated in the literature, the way a person implements the technology, takes the proper precautionary steps, and uses the correct technology to protect privacy is reflective of Bandura's (1982) theory. Bandura (1982) noted that behavior can be predicted by self-efficacy, perceived ease of use, and outcome judgments, how well an action can be executed by the individuals.

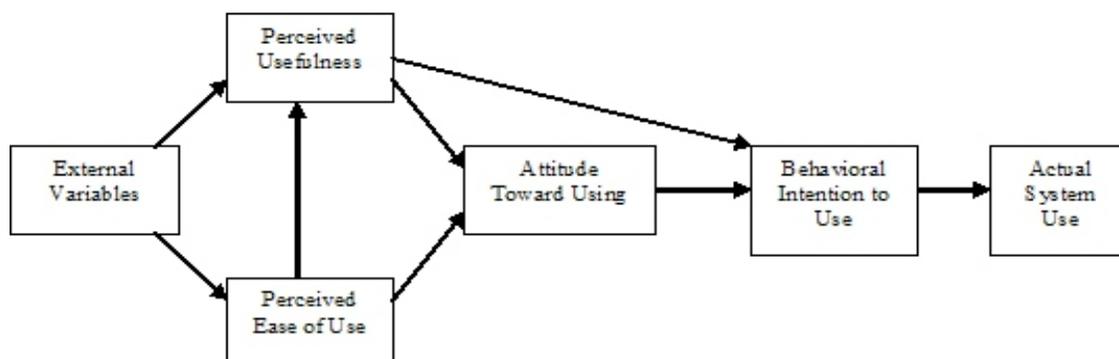


Figure 1. Technology acceptance model

Much of the literature on security management is progressive in the way that new ideas are being brought to life. One thing researchers noted is that the field is constantly progressing with new ideas to keep information safe (Gejian, 2013; Liu et al., 2012).

Literature Review

Outsiders can easily intercept wired and wireless information, which is a real concern for organizations (Manikandan et al., 2013). Although many security systems are designed for wired networks, far more security challenges exist in wireless networks than in wired networks. Manikandan et al. (2013) posited that in wireless network, communications take place using radio frequencies over airwaves, which increases the risk of interception more so than with wired networks. This means that if the message is not encrypted, attackers may modify the contents of packets during transmission.

Gregor and Krone (2006) maintained system access is the main difference between wired and wireless networks. Wired networks have physical connections; whereas, wireless networks are accessible through wireless access points (hotspots),

meaning that an unsecured wireless network is extremely susceptible to unintentional or deliberate intrusion. Many organizations install wireless communications and devices for convenience, flexibility, and ease of use. Users can move their laptop computers from one place to another while maintaining connectivity with the network (Moorthy & Sathiyabama, 2012; Radack, 2013; see Table 1).

Table 2

Types of Wireless Connectivity

Abbreviation	Name	Example	Distance
WWAN	Wireless wide area network	Users' mobile phones	10 km
WMAN	Wireless metropolitan area network (IEEE 802.16)	Internet at broadband speeds connections in suburbs of city	1 km
WLAN	Wireless local area network (IEEE 802.11)	Connectivity on the floor of a building connecting all workstations and servers	100 m
WPAN	Wireless personal area network (Bluetooth, Infrared)	Connectivity for various products and devices	1 m

Note. Adapted from Trusted Information Sharing Network (2006). Note that terminology varies and further technical variations exist within each of these categories.

As shown in Table 1, wireless connectivity can occur in a number of ways.

WLAN (IEEE 802.11) is presently viewed as the most common wireless standard, which operates in a license-free spectrum. Extensions of the standards are 802.11b, 802.11g, 802.11a, and 802.11n. The 802.11b operates in the 2.4 GHz range and provides data rates up to 11 megabit per second (Mbit/s). The new generation standard is the IEEE 802.11n, designed to improve networking over the previous standards (Xiong et al., 2011). The

IEEE 802.11 series of standards provide higher access speeds with each generation. The maximum raw data rate from 54 Mbit/s to 600 Mbit/s increases significantly with the use of four spatial streams at a channel width of 40 MHz.

WLANs are extremely popular and many corporations and homeowners are avoiding the wired expenses and delays associated with installing wired networks (Moorthy & Sathiyabama, 2012). Nonetheless, anyone with a wireless device in the close range area can intercept data being transferred unless the network is secured (Vakil, 2005). Such interception leaves the organization exposed to serious damage (Siponen, Mahmood, & Pahlila, 2009). These breaches can irreparably harm an organization by wiping out computers hard drives, or freezing computers, which causes businesses to lose potential revenues and possible leaking corporate confidential information.

WLANs networks offer wireless access to data rates of 1 mbps or more for both indoor and outdoor applications (Dhull & Singh, 2010). Wireless networks allow users to share data among users with compatible devices such as printers and other handheld devices. Many public businesses, such as McDonald and Starbucks offer wireless access to their customers free of charge, and wireless communications can help organizations cut their wiring costs (Dhull & Singh, 2010).

Wireless networks consist of basically four components for data transmission, which include radio frequencies, access points for connection to the organizational network, the actual mobile devices (e.g., laptops, cell phones, and the human element, the end users (Gregor & Krone, 2006). Each is a source for possible attack and can compromise the fundamental security objectives of confidentiality, integrity, and

availability. This means is that prior to establishing wireless networks and mobile devices, the organization IT managers should consider the risks involved and take steps to reduce and maintain an acceptable level of risk by setting up risk management. This process would allow managers to some cost-effective protection for the application of new technologies.

Ammari, Ghallali, El Kalam, El Hami, Ouahman, and El Ouahidi (2014) argued that in recent years, the evolution of iPhones has multiplied dramatically due to enhanced sophisticated features, applications, and the miniature size of portable devices. People using mobile devices can surf the Internet and exchange data. Consequently, many of their features have triggered serious security issues.

Ammari et al. (2014) sought to develop security guidance and process for mobile phones that met the anticipations of users by restraining the distribution of malware via SMS / MMS and emails. The phases entailed investigating, classifying, and safeguarding traffic in the mobile networks. They began by a developing the MPSS (Mobile Phone Security Scheme) Framework that increased the level of data security across the network of the telecommunications operator and reduced the risk of problems related to mobile devices, such as loss of data users (individuals, companies). The primary objective is to provide ameliorate security against the risk of information leakage due to malware, and to address the enigmas previously stated.

The MPSS consisted primarily of four modules. They are the following:

- *Module 1: Strategy and policies.* Create all mobile security policies aimed to decrease the probability of attacks via malicious software that disseminate via SMS / MMS or email.
- *Module 2: Security of mobile telephony and integrity.* This characteristic will enable the telecommunication operator to ameliorate comprehend the make-up and occurrence of malware by locality and cycle.
- *Module 3: Security Audit.* Every cell phone is scanned when the cell phone battery is charging for vulnerabilities and threats. This evaluation is conducted by a built in security system in the mobile phone operating system installed during manufacturing.
- *Module 4: Warning system.* The cell phone provider should notify the customer in real time of the security status of their mobile device. The owner of the mobile device should then start a system's built in security scan from their cell phone.
(Ammari et al., 2014)

It is important to note that the design and implementation of this framework will encompass the node support, the selection of routers and switches, the site of servers and components of security, and the needed instruments necessary to execute the test and evaluate the inclusive scheme of the MPSS Framework.

Wireless Security Threats and Issues

Security remains a major problem associated with wireless networks because of easy access compared to wired networks. Businesses announce their services so that potential customers can link up and use the services provided by the business. Still,

individuals in the vicinity can intercept these frequencies with wireless devices. As a result, if not properly configured, the signals can be located and monitored quite readily (Vakil, 2005).

Another security problem involves rogue access points, which can be purchased and connected without authorization to a business or home network. Rogue access can pose great security risks because of a lack of market protection against these kinds of attacks. The main risk is that these standards do not provide a way to secure data in transit against eavesdropping. Many home computer users may not be aware of the risks posed by wireless networks.

Businesses as well as home users enjoy the benefits that wireless networking provides, such as cost effectiveness, flexibility, and easy to use. With the mandate for wireless connections comes an increasing concern regarding the security and protection of the wireless networks from threats and vulnerabilities (Fenz, Ekelhart, & Neubauer, 2011). Security threats are physical and virtual in nature, which if unprotected can lead to attacks such as pilfering of information, distortion, and computing hacking (Gregor & Krone, 2006). Human threats can be accidentally or deliberately to existing vulnerabilities and are mainly caused by human factors or errors (Fenz et al., 2011; Greengard, 2013). These errors are usually committed through mishandling of confidential data and violations of industry and government regulations.

Wireless networks are typically more susceptible to security attacks than wired networks, due to the broadcast nature of the transmission medium (Mashhour & Saleh, 2013). Most network threats come from the obliviousness of users, the reserved mindset

of corporations, and the lack implementation of security features by wireless devices manufacturers (Loo, 2010). Insufficient training materials or support for users' wireless connections off site and in public places increase exposures to wireless systems security breach by external intruders.

Security and Information Security

Mohamad, Zakaria, and Nabil (2013) argued that the terms *security* and *information security* are different concepts. Security is a process undertaken to reduce risk or threats that can expose or place an organization in a vulnerable position, whereas, information security is an established business requirement to protect the organization's confidentiality, integrity, and availability of costly assets. Although definitions may vary, the most important feature of information security is protecting information assets from open disclosure, integrity violation, and denial of service. To ensure appropriate measures and to help minimize the internal security threats and risks, managers need to be knowledgeable of the elements of information security.

Information Systems Security Risk Management

It is estimated that personnel inside the organization make at least 50% of all breaches to IT systems security through unauthorized system access (Gordon, Loeb, Lucyshyn, & Richardson 2005). In the *2011 Benchmark Study on Patient Privacy and Data Security* report, senior-level employees were interviewed at healthcare facilities for getting information on data theft and loss. This benchmark study was from the Ponemon Institute. ID Experts was the sponsor (Research Information Ltd., 2011a). The prices for such breaches are approximately between \$4.2 and \$8.1 billion each year. Personal

medical data are compromised for millions of patients, and the main cause of these breaches is mistakes from employees. In spite of policies, data breaches are rising 32% in recent years and compromised patient records are at 46%. ID experts found that 55% of healthcare organizations are not confident or are only somewhat confident that they can identify these invasions of privacy. Regarding people who are not confident they can even locate these data physically, that number is 61% (Research Information Ltd., 2011a).

Added to this serious dilemma is the outsourcing of many services both medical and administrative to third parties. These third parties have made many mistakes in relation to data breaches. A full 49% of the participants related that stolen or lost computing or data hardware contribute the most to events involving data breaches (Research Information Ltd., 2011a). Many negative issues are present in the healthcare industry that can lead to medical identity theft among other problems. Some of them are (a) The fact that over 80% of healthcare organizations collect, store, and send data via mobile devices, yet more than 50% of the participants revealed that they do not protect the data on the devices. (b) In spite of new government regulations and policies, breaches are virtually unaffected. (c) Healthcare organizations report that they often lack the resources or the finances or good procedures and policies to prevent breaches. (d) Data breaches leading to medical identity theft were reported by 29% of respondents, a 26% rise since 2010 (only one year earlier than the report). Although 90% of the respondents acknowledge the harm that data breaches can bring to patients, only 25% monitor

services after the breach; and (e) it is the patients, 35% of the time, that have to report the breach (Research Information Ltd., 2011a).

Research Information Ltd. (2011a) cited Rick Kam at ID Experts, who suggested the following three steps to minimize security risk management:

1. Inventory all elements of personally identifiable information whether electronically or on paper to see how data are used, collected, and stored.
2. In order to meet HIPAA and HITECH regulations, an incident response plan can be prepared to confront data breaches. Each employee's responsibilities, actions, and roles are designated in the plan.
3. Organizations must review the agreements, contracts for all business associates so that they comply with regulators, and are consistent in managing Protected Health Information in healthcare.

Hu, Xu, and Dinev (2011) posited that hacking, for both individual PCs and corporate systems has gone from sport to organized criminal actions to control significant profits. The impact of these crimes costs over \$1 trillion annually. Still, in spite of preventive efforts, people are “the weakest link in the defense against outside attacks and the most dangerous to the organizations within” (p. 54). Hu et al. argued that humans also develop preventive methods including procedures and policies in addition to regulations from the government because humans know the most, intimately, about permissions (given to them or taken by them) and organizational systems. Hu et al. conducted their research via a survey of employees from five big Chinese firms.

Hu et al. (2011) found that “individuals with low self-control are more likely to be tempted by the appeal of the violations in terms of perceived benefits and thus more likely to commit the acts” (p. 59). Hu et al. found that deterrence because of the presence of many individuals with low self-control does little to lesson violations of policy. They also found that rational choice for deviant behavior was supported; perceived benefits overrule perceived risks. As a result, Hu et al. recommended that because deterrence was overruled by low self-control, firms can lower violations of policy by doing screening for employees who exhibit high more standards and self-control to avoid self-centered individuals with low self-control. According to the 2007 Global State of Information Security Study by Price Waterhouse Cooper, insiders commit 69% of database breaches, the opposite of what has been believed in the past – that hackers compromise database security (Aldhizer, 2008). Therefore, those who audit organizations usually recommend the use of firewalls to prevent hacking. However, because the biggest threat is from employees and third parties, such precautions would do little.

A study done by InformationWeek.com found that 45% of employees who are trusted by their supervisors confessed to taking sensitive data with them when they left the organization. Aldhizer (2008) emphasized that internal auditors refocus their attention on internal risks. One suggestion is to use “centralized and automated identity and access management (IAM) controls ... to enforce security policies by monitoring employee and third-party access and use of sensitive data” (p. 71). These steps need to be taken “in real time across multiple databases in numerous locations” (p. 71). Siponen, Mahmood, and Pahnla (2009) argued that careless employees can create serious threats to their

organizations when they do not follow information security policies. Their survey research suggested that if employees realized how vulnerable their organizations were to security threats, they would more likely to comply with information security policies or demonstrate intent. Siponen et al. (2009) reported that an overwhelming majority of company own employees frequently violate security policies and pave the way for such breaches.

Wireless communications, coupled with high risk for unauthorized users with access to the computer networks, dictate the need for greater measures to be taken to protect sensitive information and the assets of the company (Mashhour & Saleh, 2013). In taking such measures, organizations should encourage and enforce safe practices through education (Loo, 2008). Successful management of security risk program requires communicating to all users and providing education about potential threats and vulnerabilities to the organization (Chenoweth, Minch, & Tabor, 2010). In placing more emphasis on identifying employee related threats, the occurrence of security breaches may lessen. People, policies, and processes are real sources of vulnerabilities and should be an active part of security risk management.

Users

Mohamad, Zakaria, and Nabil (2013) maintained that all users from IT personnel to top management are the end users. A user is defined as anyone who accesses any information and communications technology asset, such as employees, administrative personnel, contractors, or vendors. IT personnel includes security managers, security administrators, analysts, security staff members, and security officers. Mohamad,

Zakaria, and Nabil (2013) claimed that all users' knowledge is based on their roles and responsibilities regarding their work. The premise is that every employee needs to know the importance of information security in order to protect and preserve valuable sensitive information and the assets of the organization. What this implies is that to avoid human error, all users must have the appropriate behavior and knowledge of information security. These components should be aligned so that the associated risk of information security in organization can be achieved (Mohamad, Zakaria, & Nabil, 2013). (See Table 2)

Aldhizer (2008) recommended that when users leave the organization their accounts pose insider risks. One organization that Aldhizer uses as an exemplary organization is Wellspan, a healthcare network in York, Pennsylvania. The organization checks for files that have not been accessed within the last two or three months and see if they may be deleted. They experienced delays but mitigated the problem by using an automated link between human resources and the TAM system the day after the employee leaves the organization. WellSpan's IAM system records all accounts accessed by all users the entire time of their employment. The company especially monitors accounts that users creates during their last few weeks of employment, which are more apparent to include data that employee may purposefully remove from the organization.

Because employees tend to send sensitive data via email, all messages are scanned for rich information, which can be deleted. Because outgoing employees can use paper and pen to record sensitive information, the risk is mitigated by recording login and logout times and access frequency in real time. If the frequency and duration of accessing

sensitive files rises suddenly, the forensic team is called in to investigate. Another insider problem involves third parties. Thus, Wellspan will not permit these parties to access internal networks, but instead can only access known as a demilitarized zone, an isolated network situated between the Internet and the organization's internal network that stores regularly requested data. Moreover, the IAM controls are in place to make sure separately tagged sensitive data are not uploaded to the demilitarized zone, and third parties cannot have email accounts through the organization (Aldhizer, 2008, p. 73.).

Table 3

Categories of Users

Users	Necessary information security knowledge
End users	Strong password creation and protection Computer viruses and safe use of email
IT personnel	Knowledge of Information Security and technical controls
Top management	Knowledge on security policy and procedures, user training and education

Table 2 provides a summary of the minimal knowledge needed for users at all human levels in the organization. Loo (2008) suggested several measures that corporate officers should consider: (a) educating their employees through professional seminars, (b) encourage vigilance in reporting suspected intruders as soon as possible, and (c) teaching employees how to turn on common security features of their routers. Loo (2008) acknowledged that it is virtually impossible to make computing safe because too many basic weaknesses exist in new technologies and routers.

Federal Trade Commission (FTC) Standards and Enforcement

In the aftermath of many major organizational security breaches, the FTC became more involved in the security of personal data. The FTC is a law enforcement agency with authority rendered under the Division of Privacy and Identity Protection to enforce data security and fine companies that do not institute reasonable safeguards (Rhodes & Kunis, 2011). The sensitivity of the data and the costs of avoiding potential risks determine the reasonable standard. Companies should commit to time and financial resources, not only to avoid data breaches, but also to prepare for damages, which may result (Rhodes & Kunis, 2011).

Weise (USA Today, 2014) reported a Russian data breach involving a crime ring, which amassed a supply of 1.2 billion username and password combinations. The breach was reported as the largest ever and included information from individuals and companies worldwide. This breach is just another indicator of the type of major security issues that continues to exist, despite the use of sophisticated countersecurity measures. Weise claimed that very few of those email addresses had been affected, but cautioned that although security is improving and is much more robust than was 10 years ago, things seemed to be getting worse even as security improves (USA Today, 2014).

Kirankumar, Babu, Prasad, and Vishnumurthy (2012) reported several ways to secure a wireless network from intruders. Kirankumar et al. claimed that the most effective way was encryption or scrambling of communications over the network. Most wireless routers have built-in encryption mechanisms that can be turned off and on by the user. The second suggestion was to install anti-virus and anti-spyware software and

insure that the latest version is the current version in use. The third way was to turn off the mechanism called identifier broadcasting that sends out a signal to any device in the vicinity announcing its presence. This prevents hackers from honing in on vulnerable wireless networks. United States Computer Emergency Readiness Team (2014) reported an increased threat from software attacks that take advantage of vulnerable web browsers. This problem was made worse by a number of user actions, which included (a) clicking on links without considering the risks of their actions, (b) web addresses can be disguised and take users to an unexpected site, and (c) using computer systems with bundled software packages can increase the number of vulnerabilities.

New attacks on WLAN securities forms are continually being discovered. These range from misconfigured WAP to hijacking (Dhull & Singh, 2010). It was suggested that organizations employ a security system that includes an intrusion detection system (IDS). At minimum, these could help defend and detect these potential threats. Organizations without a WLAN are at risk of wireless threats and should consider an IDS solution. Dhull and Singh (2010) cautioned that some IDS systems have limited capabilities for detecting attacks that differ significantly from previously known attacks.

Security Risk Assessment (SRA) Model

Security decisions, planning, and implementation of security measures should be based on sound SRA (Saleh et al., 2011). SRA is a process of evaluating security risks and identifying the required security measures. Saleh et al. (2011) suggested that assessment should be conducted at the earliest stage of the system development as well as when changes occur to the IS environment. In other words, to be effective, risk

assessment should be an ongoing process. The process includes identifying the threats and vulnerabilities that could gain access to confidentiality, integrity, and setting controls required to manage the risk.

Other Studies and Methodologies on Wireless Security

The primary research question of this study queried how IT managers identify and manage the security threats associated with wireless networking in the IT organization as measured by the SRA and management model. This question forms the basis for investigating and assessing the security measures organizations take to protect the confidentiality and integrity of the business. Although IT administrators may already be aware of the proper techniques for securing the WLAN itself, the measures they take to protect the organization from wireless threats is unclear.

Many studies reviewed addressed security breaches in various organization or business industries. These include, but are not limited to, the healthcare industry, government, education, and financial institutions. Tiong, Hafeez-Baig, Gururajan, and Soar (2006) explored users' understandings of security issues associated with wireless technology in the healthcare industry situated in Australia. They used a mixed research method to investigate user interests for wireless technology and security requirements in the healthcare industry. The study was conducted in two phases: exploratory and confirmatory. Participants of the focus group (first phase) felt that any security measures of wireless LAN should be beneficial to their work. The conclusion drawn was that healthcare workforce was organically mobile in performing their daily work functions.

Using wireless technology combined with robust security features would bring benefits to work.

Based on these findings, Tiong et al. (2006) hypothesized that using wireless technologies in healthcare organizations that could impact the design of the business, economic performance, and the working conditions of staff. Tiong et al. emphasized the importance of assessing IT risks in the health-care industry. Tharp (2008) states assessing general IT control and high-risk areas can better enable auditors to address key security issues in the health-care sector.

Chenoweth, Minch, and Tabor (2010) reported that approximately 60% of all wireless networks use no form of encryption and often used aging technology with several security weaknesses. The problem was more evident with public hotspots, because consumers seemed more interested in ease and convenience of use than the level of security. Wireless consumers who connect with many different public access points increase their chances of picking up malicious codes, which in turn are easily transferred to wired networks.

Chenoweth et al. (2010) conducted a study on a university campus to explore wireless consumers vulnerabilities and security practices and determine the number of computers that were not adequately secure. The aim was to investigate precisely how well wireless consumers secured their computers and the risk level associated with wireless networks. Data collection was performed continuously with 3,331 computers access to the wireless network for 41 days. The data collection process entailed of two essential constructs: *device detection* and *vulnerability scans*. User vulnerability scans

were performed using Nmap, a tool for port scanning. The results indicated that an distressing number of wireless network consumers were not using a firewall (9.13%) and had detectable open ports (8.62%), leaving them vulnerable to outsider attack. Various forms of malware compromised several computers Chenoweth et al. (2010).

The outcome of the study was significant implications for business without the resource to deploy automated assessments products. Chenoweth et al. (2010) suggested that using the scanning technique as in their study would strengthen organizational policy. Consumers would be made aware that they can be audited, and are more likely to remain compliant. Organizations are aware that if they are not compliant, their information is not safe. The technique is easily replicated and is noninvasive in terms of individual privacy (WatchGuard, 2013).

Teer, Kruck, and Kruck (2007) presented the results of a study involving the security practices and perceptions of students majoring in computer information systems and related technology courses. Students' were questioned about their usages of various antivirus programs, firewalls, opening attachments, password security, and security patches. The researchers found that 28% of student participants either did not or were uncertain if they consistently installed updates to their antivirus software. Forty-seven percent of the students reported one or more viruses during the past twelve months. The majority of respondents (73%) stated that they did not validate the sender of an email before opening an attachment (Teer et al., 2007).

Those results indicated students are leaving their personal computers vulnerable to viruses. The combination of these two responses may point to a general lack of

knowledge among students on both the need for home computer security and how to protect their home computers better. However, when students were asked to respond to the importance of computer security for business, they responded almost unanimously that it was important (Teer et al., 2007).

The significance of this study was that the university should do more to assure that students in the campus workplace are not bringing unsafe computer practices to the corporate environment and to a university environment. Vulnerability is growing in corporate computer information systems. The threats to the security of personal computers, dictates that those responsible for curriculum in all programs throughout the university should ensure that students are obtaining an adequate level of understanding and skill on the fundamentals of computer security. Internal user practices and human factors focusing on end user perceptions and attitudes leading to behavior are identified as critical elements for understanding how to move forward with IT security (McCafferty, 2010).

Warner (2011) conducted a cross-sectional study to examine student's perceptions of the environment and the meaning they applied to their experiences with the environment. The study was described as a psychological climate research. The participants were university 259 students responsible for the IT security on the computer they used to in the workplace to perform data processing (Warner, 2011). The findings indicated that students believing they were in a safe and positive work environment were more driven to participate in safe activities than students who felt they were not. The researcher concluded that awareness, attitude, and behavior were important human

factors that should be considered to gain understanding and knowledge of users' experiences regarding IT security (Warner, 2011).

Butt (2013) reported the findings from a survey of security approaches for wireless ad-hoc networks in wireless technologies known as *ad-hoc networking*, commonly used when users use Bluetooth, IEEE 802.11 technologies. Mobile users participate in setting up the network for communication within the range of the wireless link. Butt (2013) argued that security is just as critical and important in ad-hoc networks as in traditional networks and that sensitive data should be protected from malicious eavesdroppers and network services should only be provided to eligible users. Many different approaches can be used in order to achieve security-aware routing in wireless ad-hoc networks as shown in Table 3 that follows.

Table 4

Secure Aware Routing Properties and Techniques

Routing Properties	Techniques
Authenticity	Password, certificate
Authorization	Credentials
Integrity	Digest, digital signature
Confidentiality	Encryption
Nonrepudiation	Changing of digital signatures
Timeliness	Timestamp
Ordering	Sequence number

Note. Adapted from S. Butt, A survey of security approaches for wireless ad-hoc networks, 2013. *Golden Research Thoughts*, 2(9), pp. 1-10.

Farahmand, Navathe, Sharp, and Enslow (2005) argued that before managers can determine how much time and resources are needed for a security strategy, they should know what type of attacks may threaten the networks and the departments connected to that network. The most common types of attacks described were the following:

- *IP spoofing attacks:* A hacker steals an authorized Internet Protocol (IP) address, which is a unique address. The hacker determines the IP address of an idle computer when no one is using that computer, and then uses the temporarily inactive IP address.
- *Packing sniffs:* The hacker listens to Transmission Control Protocol/Internet Protocol (TCP/IP) packets and steals the information, which includes user logins, e-mail messages, and credit card numbers.
- *Password attack:* The most common weak-point in any system. Hackers generally find a user with an easy password or use a special program, which cycles through a range of words from a dictionary.
- *Session hijacking attacks:* The hacker taps into a connection between a client and a server. The hacker then simulates the connection by using its IP address (Farahmand et al. (2005)).

The main premise of this report was that both businesses and consumers benefit when wireless networks and devices are safeguarded. Applying the appropriate wireless risk analysis can reduce specific threats and vulnerabilities. While these measures cannot

prevent all infiltrations, they can be effective in reducing many of the common risks associated with wireless technology.

Summary and Conclusions

The previous sections provided valuable insight into the risk and chances of threats that can penetrate information systems and subsequently cause tremendous losses and or damages, which effect an organization directly or indirectly. It is important for IT managers and users to understand the attacks that might affect the WLAN. To avoid the adverse effects, IT organization should apply risk analysis in wireless threat management. When risk analysis is applied as an effective tool, security policies can be developed and applied to guard the WLAN against internal and external attacks. Continuous monitoring and periodic testing should be employed to verify that a deployed WLAN meets defined objectives (Phifer, 2008). The vulnerabilities previously noted are exposed and the appropriate fixes can be applied. This process of risk analysis is illustrated in the following diagram (see Figure 2).

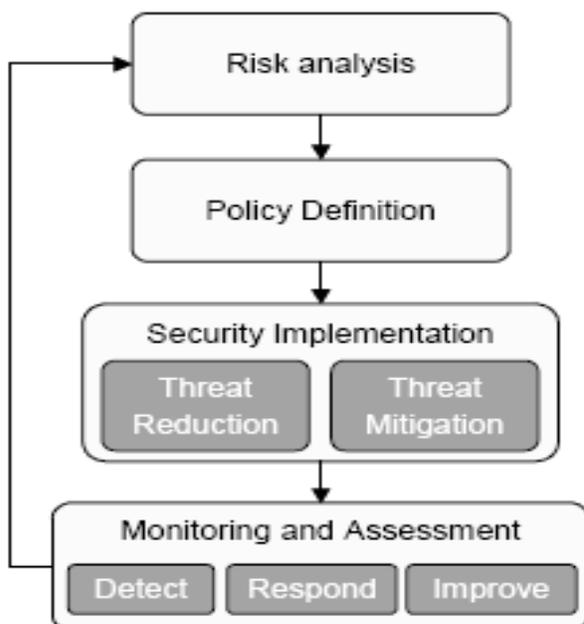


Figure 2. Security as a process (Phifer, 2008).

Phifer (2008) noted that understanding the vulnerabilities and attacks that can occur within the organization is crucial; however, some attacks are more damaging than are others. Phifer indicated that regardless of what countermeasures are applied, it is not feasible or attainable to defend any organization or business against all of the countless conceivable attacks; suggesting that a more realistic objective is to decrease the associated risk to a more acceptable level. A good first step is to begin by identifying one's own wireless vulnerabilities and possible attackers.

Steps in Performing Risk Analysis

An organizational IT manager should follow several steps considered necessary in performing risk analysis as recommended by Phifer (2008). They are the following:

- Define the business needs of the organization.
- Identify and certify who needs wireless networking access and where.
- Carefully classify individuals or departments allowed to use 802.11 in the workplace and with mobile devices off site.
- Regulate which applications and databases should be accessible to wireless Users. (Phifer, 2008; Radack, 2013)

Aside from these key steps, the IT manager needs to assess and quantify any new risks to the business that may be caused by adding wireless networking. That is, managers should estimate the potential cost to business during downtime and recovery expenses.

Base on the risk analysis outcome, the manager is able to write and implement enforceable security policies (Radack, 2013).

Vulnerability assessment. Another type of assessment that may be used to identify security weaknesses and risks is the vulnerability assessment proposed by Phifer (2008). The primary purpose is to evaluate and determine the severity of and the necessary steps to reduce or eliminate the security threats. Phifer (2008) argued that to be truly useful, assessments should be performed recurrently to detect new vulnerabilities and to confirm that installed security measures are functioning as intended. These assessments may be conducted internally or by independent persons who are knowledgeable or have no knowledge of the organization's security networks. The premise is that organizations and individuals reap benefit when wireless networks and devices are protected from deliberate and intentional threats. Again, it is important to stress that although no perfect system exists that can prevent all penetrations; countermeasures can offer some managerial solutions to reduce many common risks associated with wireless technology.

Managerial solutions. The literature reviewed clearly indicated that wired networks compared with wireless networks might be more vulnerable and easy to attack (Kirankumar et al., 2012). In a wired network, hackers or attackers gain access by penetrating some physical security perimeter to gain network access, whereas, in wireless networking, attackers easily gain access without getting into a building or physical setting. However, the literature indicated that wireless security is not solely a technical issue, a human factor is also present (Guo, Yuan, Archer, & Connelly, 2011). These

factors must be addressed by appropriate countermeasures that involve employee awareness of the issues, user education, clearly stated organizational policies, and practices by management.

Taylor and Brice (2012) argued that too often when managers make security decisions, they do not always have the requisite expertise regarding threats to their businesses' data. Consequently, they end up relying on only information readily available and a technology-based approach to addressing organization security risks. Taylor and Brice (2012) noted that most managers turn to trusted advisors, whom they consider as the experts to protect the organizational from security breaches (example, the Information Technology (IT) manager). The premise is that if management relies solely on this advice, the human element of organization security management may go unnoticed.

The data from a case study conducted by Taylor and Brice (2012) revealed that the perceptions of managers were significant factor in risk causing behavior of employees. Therefore, management should not rely solely on technology-based countermeasures and ignore the human element of risk compliance. This behavior may lead to insufficient countermeasures to protect organizational information from the deliberate or unintentional risks caused by employee actions. The findings in their case study pointed to evidence that security management practices and controls are especially critical to maintaining and operating a secure wireless network (Taylor & Brice, 2012). These practices included: (a) controlling the wireless LANs coverage area, (b) management and proper configuration of access points, (c) establishing security policies,

(d) regularly conducting security audits, (e) providing user education, and (f) controlling for physical security in wireless network facilities.

Security of information is paramount to corporations, which use wireless networks. If these corporations' networks are left vulnerable, they can suffer a variety of negative repercussions. Fenz et al. (2011) reported that organizations lose an average of approximately 2.1 % of their market values within two days surrounding security breaches. An overwhelming majority of security breaches are caused by human and system errors (Greengard, 2013).

The literature review indicated a scarcity in research on various security and risk measures from the perspective of different researchers. This gap in literature reviewed remains a vital concern. More research was needed generated from employees who have access to its resources and are familiar with the system to fill this gap in literature (Maqousi, Balikhina, & Mackay, 2013). It was unreasonable to expect perfect wireless solutions. Nevertheless, companies with wireless networks needed to ensure they were managed effectively. This means conducting regular risk assessments of their specific security needs, policies, and standards in an effort to ensure that ever evolving security needs are addressed (Cox, 2010; Hyeokchan & Sin-Hyo, 2013).

The literature reviewed clearly indicated that human factors play an important role in the wireless security breach in the organization. The end users can put the organization at risk for threats and security breaches. Conversely, humans must protect the company's assets. Top management and all users must be made aware of their

responsibilities to the organization. The focus of Chapter 3 is the research design and methodology.

Chapter 3: Research Method

Introduction

The purpose of this study was to investigate the security risk practices that IT administrators used to protect and manage the confidentiality and integrity of information in small to medium IT organizations using wireless networking. Cereola, Wier, and Norman (2012) claimed that small to medium enterprises differ from large enterprises mainly in their assignments of decision makers. Large firms typically have a Chief Technology Officer (or Chief Information Officer [CIO]) for IT decision making, while small to medium enterprises often rely on the collective IT knowledge and experience of the top management team. In any size firm, it is important for leaders to understand the security measures that managers take to protect the confidentiality and integrity of the IT organizations (Vanitha, Selvakumar, & Subha, 2013). The focus of this chapter is a discussion of the research design, methodology, population and sampling, threats to validity, and ethical considerations of this study.

Research Design and Rationale

This study employed the non-experimental quantitative survey design to examine and investigate the security practices by which managers of small to medium IT organizations protect and manage the security threats associated with wireless and wired networking in the organization. Creswell (2009) suggested that the method of a study should match the researcher's plan to address the research problem.

The quantitative research design was selected to answer two research questions and four hypothesis statements.

RQ1: What security risk assessments, if any, do IT administrators perform to protect the confidentiality and integrity of the organization's information?

H_01 : IT administrators do not regularly perform network security risk assessments to protect the confidentiality and integrity of the organization's information.

H_a1 : IT administrators regularly perform network security risk assessments to protect the confidentiality and integrity of the organization's information.

Research Question 2: Do network security risk management practices of IT administrators meet the minimally accepted practices and technical standards for wireless networking as measured by security self-assessment survey?

H_02 : The network security risk management practices of IT administrators do not meet the minimally accepted practices and technical standards for wireless networking as measured by security self-assessment survey.

H_a2 : The network security risk management practices of IT administrators do meet the minimally accepted practices and technical standards for wireless networking as measured by security self-assessment survey.

Quantitative studies attempt to report how many people are in a particular category, and they explain relationships between one category and another (Jourdan, Rainer, Marshall, & Ford, 2010).

I used the quantitative design to quantify the attitudes and opinions of IT managers and IT administrators in an effort to, generalize the results from a larger sample population of IT organizations. Quantitative data collection methods are

considered to be more structured than qualitative data collection methods. In contrast, qualitative interview data tend to be narrative in nature. A qualitative researcher produces rich, detailed descriptions in a narrative while a quantitative researcher produces data that can be coded and processed quickly (Creswell, 2009; Trochim & Donnelly, 2008). Additionally, qualitative data collection methods use unstructured or semi-structured techniques. Some common data collection methods include individual interviews, focus groups, and observations. The sample size is typically smaller, and participants are usually purposefully selected (Creswell, 2009).

Fink (2013) noted that some research requires a design, which includes no applied treatment or experiment. This method is often referred to as a *non-experimental design*. Although many possible quantitative research designs exist, the method I selected for this study is the non-experimental design. Using the non-experimental design for this study was easy to implement because in this study, I do not have to manipulate any of the variables or conditions of the study. Consequently, the non-experimental design was a good choice because the relationship among the variables was unknown and required no manipulation.

I used a quantitative survey research design primarily to generate numerical data or data that can be transformed into descriptive and inferential statistics. My data collection method was the online survey. Many researchers consider surveys as the primary method of quantitative research because of statistical accuracy. Several types of surveys can be chosen such as mail, telephone, and online. I selected online in consideration of time and cost. In this technological age, most people have computers,

especially the population that I sampled. Some researchers consider online surveys as the least expensive format and a quick way to collect data (Fink, 2013). Participants can also be recruited easily.

Methodology

Population and Sampling

The population of this study consisted of 25,000 small to medium IT organizations in the United States that were comprised of IT managers, network and security engineers, and other professionals. According to SurveyMonkey, a commercial online survey company, the sampling frame for this study was comprised of more than 1,500 IT organizations. An IT organization is defined as an organization with a division within the company that oversees the establishing, monitoring, and maintaining of information technology systems and services (Pazos, Chung, & Micari, 2013).

The sampling selection was both random and convenience sampling. Random sampling was used to select a group of participants (sample) from the larger group (a population). It is called random because each individual was selected entirely by chance and each member of the population had a known, but possibly non-equal, chance of being included in the sample. By using random sampling, the likelihood of bias is reduced (Fink, 2013; Trochim & Donnelly, 2008). Convenience sampling includes individuals who are available and willing to take the survey. The minimum sample size of 111 for this study was calculated using G*Power version 3.0 with a regression statistical test. Given the effect size of 30 (a medium effect size), alpha .05, and .95 power, the minimal sample size was calculated to be 111 (Faul, Erdfelder, Lang, & Buchner, 2007).

Recruiting Procedures

Upon approval by Walden University's Institution Review Board (IRB), the sample for the study was obtained from a commercial online database produced by SurveyMonkey and disseminated by email invitation. According to the administrator of SurveyMonkey, its service relies on informational sources obtained from databases comprised of members from directories, new business filings, press releases, corporate websites, and user-generated feedback. The sampling frame is comprised of more than 5,000 members. The database is populated with members from organizations, which include but are not limited to the National Institute of Standards and Technology, Toastmaster International, Career Field Information Resource Management Level II and III certified from the Federal Government Acquisition Workforce, and members of the commercial business sector.

All data collected were stored on the hard drive of a secured computer and all data files are password protected and will be retained for the required period of five years. At the completion of this period, I will erase and properly delete the surveys from the hard drive of the secured computer.

Instrumentation

Instrumentation was developed replicating previously validated web-based questionnaires to test the hypotheses. The instrument is entitled *Securing Personal Information: A Self-Assessment Tool for Organizations* (see Appendix A), previously published by Office of the Information and Privacy Commissioner for British Columbia, (2012). The instrument is comprised of 17 key categories or constructs for assessment;

however, only six constructs were used in the present study: (a) risk management, (b) physical security, (c) systems security, (d) network security, (e) wireless, and (f) data integrity and protection.

The authors of the instrument noted that reasonable safeguards in the organization should include several layers of security. These safeguards should include, but not be limited to, risk management, security policies, human resources security, physical security, technical security, incident management, and business continuity planning (Office of the Information and Privacy Commissioner for British Columbia. 2012). Each category contains several questions or items. The items on the instrument were color-coded blue by the author, which indicated the minimum-security requirements for any organization regardless of its size. The remaining questions were color coded in black indicating that organizations should raise their security standards beyond those minimum levels. The authors of the instrument maintained that the goal of the survey was for each participant to be able to answer “yes” to each question.

Operationalization

Six constructs (independent variables) and two-outcome variables (dependent variables) are central to this study. The independent variables (risk assessment practices) were defined by the six constructs being assessed as measured by the self-reporting survey instrument developed by the Office of the Information and Privacy Commissioner (2012) of Canada. The constructs are: (a) risk management, (b) physical security, (c) systems security, (d) network security, (e) wireless, and (f) data integrity and protection.

Each construct represents the generally accepted security practices and technical standards that organizations employ. The constructs serve as tools for organizations to evaluate their information protection readiness and performance. Each of the constructs has several items that were scored as categorical data: risk management (17), physical security (17), systems security (19), network security (7) wireless (15), and data integrity and protection (15), for a total of 83 items (See Appendix). The following section presents an example of the type of survey questions asked:

- Has the organization identified what personal information assets are being held and their sensitivities?
 - Do physical security measures used for storing personal information include:
 - Locked cabinets? Locked office doors?
 - Are terminals and personal computers used for handling personal information positioned so that unauthorized personnel cannot see their screens?
 - If a user walks away from his or her terminal, does an automatic process exist to lock out all users after a defined period of inactivity? (Office of the Information and Privacy Commissioner for British Columbia, 2012).

The Office of the Privacy Commissioner of Canada (OPC Privacy Policy), (2012) granted full permission for noncommercial use. In sum, it stated that:

Individuals may reproduce the materials in whole or in part for noncommercial purposes, and in any format, without charge or further permission, provided the user exercised due diligence in ensuring the accuracy of the materials

reproduced.” The user has to state the complete title of the materials reproduced, as well as cite the author (OPC Privacy Policy, 2012).

Compared to other questionnaires, this survey fulfilled three basic requirements as follows: (a) the survey was prepared for self-administration, (b) participants were able to complete survey in 15 minutes or less, and (c) the use of yes and no responses made the survey easy to understand and complete. All were scored as categorical data. At the end of the surveys, all data were reviewed and inspected for missing data. Fink (2013) stated that it is reasonable to expect some data would be missing. Data from the surveys were analyzed using the Statistical Package for the Social Sciences (SPSS).

Data Analysis Plan

To recapitulate, this quantitative research design addressed two research questions and four hypothesis statements.

Research Question 1: What security risk assessments, if any, do IT administrators perform to protect the confidentiality and integrity of the organization’s information?

H_0 1: IT administrators do not regularly perform network security risk assessments to protect the confidentiality and integrity of the organization’s information.

H_a 1: IT administrators regularly perform network security risk assessments to protect the confidentiality and integrity of the organization’s information.

Research Question 2: Do network security risk management practices of IT administrators meet the minimally accepted practices and technical standards for wireless networking as measured by security self-assessment survey?

H_02 : The network security risk management practices of IT administrators do not meet the minimally accepted practices and technical standards for wireless networking as measured by security self-assessment survey.

H_{a2} : The network security risk management practices of IT administrators do meet the minimally accepted practices and technical standards for wireless networking as measured by security self-assessment survey.

All data were collected for the study via Internet using SurveyMonkey, an online commercial database. To begin, I uploaded the self-assessment tool online. I uploaded an introductory letter explaining the purpose of the survey, a description of the role of the participant, explanation of how the data were used, and an estimated time to complete the survey. Participants interested in the study were directed to the web-link to read the consent page. Continued participation implied consent, as all responses were anonymous. No direct contact was made with the participants. The self-assessment tool took approximately 10 minutes to complete.

The surveys were self-administered using random sampling. Using random sampling, each participant had an equal chance of being selected for the study (Fink, 2013). Participation was strictly voluntary and the participants could have discontinued or exited the survey at any time without penalty. Because of time constraints and the survey design, follow up or exit interviews were not conducted. Once I collected the survey data

from participants, the next step was to perform the appropriate statistical analyses, interpret the data, and begin writing up the results.

Several steps were taken in data analysis. These included coding the survey data, uploading to SPSS, doing basic analysis, and testing the hypotheses. Data analysis included both descriptive and inferential statistics. Descriptive statistics is a commonly used analysis method for survey research, which includes numbers of frequencies, percentages, and measures of central tendencies (Trochim & Donnelly, 2008). Inferential statistics is concerned with making predictions or inferences about a population from the sample.

Coding is the process of assigning numeral or character codes to all responses for each question in the survey (Creswell, 2009). I began by printing off a hard copy of the data and checking to make sure that all entries were correct. As a convention, I entered the code Yes = 1 and No = 2. I then assigned a name to the variables. For example, all blue areas on the survey sheet indicated the minimum-security requirements for any organization; whereas, the remaining questions could help organizations raise their security standards beyond those minimum levels. Therefore, the output variable was the labeled as the minimum-security requirements. These responses were analyzed to address research question two, which examined whether the network security risk management practices of IT administrators met the minimally accepted practices and technical standards for wireless networking as measured by security self-assessment survey (see Table 4).

Data analysis for this survey research involved computing and reporting frequencies, means, and percentages in table format. The descriptive statistics included computing the mean and standard deviation. The questions on the survey had only two possible response options which were Yes/No, which is considered a binary or dichotomous) response variable. The responses were analyzed as categorical data type. All responses were tabulated according to the minimum and non-minimum categories as coded in blue.

Statisticians have devised and reported a number of ways to analyze and explain categorical data. The most frequently used technique for analyzing categorical data is the Chi-square test for independence (Fink, 2013). The chi-square test was used in this study to determine whether a significant difference was present between the expected frequencies of the IT participants and the observed frequencies in the yes/no categories. When using Chi-Square, the researcher should use only numerical data, have at least one or more categories, use simple random sampling, and have an adequate sample size of at least 10 (Fink, 2013). All data were entered into SPSS.

Threats to Validity

As in any research, known threats to validity and reliability existed. I accepted and applied procedures adopted by Walden University's IRB. I provided appropriate explanations and justifications for actions taken during the survey, which included describing the data accurately and following sound research methods and procedures. A common threat that may be noted involves internal validity, which is concerned with the rigor of the study design (Fink, 2013). The degree of control exerted over potential

extraneous variables determines the level of internal validity. Using random sampling helped to minimize this risk and effectively control all threats to internal validity (Fink, 2013).

Prior to wide distribution of the survey, SurveyMonkey's web administrators reported that survey was pre-tested by five members in their organizations' database who met similar criteria of study participants any necessary adjustments were made to facilitate clarity and understanding of the six constructs. The internal validity of the constructs was measured using Cronbach's alpha coefficient, which represents the reliability of the measurement scale for the constructs. A coefficient greater than 0.7 represented satisfactory reliability and was considered satisfactory.

Ethical Procedures

Whenever research involves human subjects, the survey researcher needs to be attentive to the ethical manner in which the research is carried out (Fink, 2013). The key ethical issues that were considered in this study were data management and data protection. Data were collected in an ethical and reliable manner, which did not cause or produce harm to participants. Participation in the study was completely voluntary. Participants had the option to discontinue participation in the survey at any time. Participation and all responses were confidential. Only the researcher can have access to individual responses. The potential risks of the research include the researcher not having control over the participants' environment, participants being uncomfortable in answering questions.

Table 5

Research Questions/, Survey Questions, and Analysis

Research questions	Related survey questions	Type of analysis	Explanation
RQ1: What network security risk assessments, if any, do IT administrators perform to protect the confidentiality and integrity of the organization's information?	Questions 1.1-1.7	Descriptive Statistics Inferential Statistical	Examine Risk Management, which includes risk treatment and reviews of the organization.
	Questions 6.1-6.19	Descriptive Statistics Inferential Statistical	Examines System Security which includes terminals and personal security, mobile devices.
	Questions 12.1-12.8	Descriptive Statistics Inferential statistical	Data Integrity and Protection
RQ2: Do network security risk management practices of IT administrators meet the generally accepted practices and technical standards for wireless networking as measured by security self-assessment survey?	Questions 7.1-7.7		Examines the entire system of transport and storage technologies.
	Questions 8.1-8.15		Examines use of handling of personal information using wireless networks

Before the data were collected, I obtained approval from Walden University's Institution Review Board (IRB). On approval by IRB, participants were invited to participate in the survey distributed by SurveyMonkey. The consent form contained statements of (a) purpose, (b) procedures, (c) potential risks, (d) potential benefits, (e) confidentiality, (f) participation and withdrawals, and (g) personal identification of the researcher.

I provided written instructions to the participations that this study was strictly voluntary and at any time during the survey, he or she could change their mind and could terminate the survey any time. Participants' names or any other identifying information were not reported in the study. All electronic survey data and printed documents were stored in a locked file cabinet in my office where only I have access. All information stored on my computer was password protected. All data will be deleted from computer hard drive or shredded in 5 years. Because the study was anonymous, participants were not required to sign consent forms. The participant's completion of the survey implied consent.

Summary

In Chapter 3, I provided the research design and data collection process for this non-experimental quantitative study. I summarized arguments in support of using qualitative research with categorical outcomes. The purpose of this non-experimental quantitative study was to investigate and determine the security risk assessment practices IT administrators use to protect the confidentiality and integrity of the organization's information. The data collection method for this study was a self-reported, web-based

survey method using a cross-representation of industries and company sizes.

SurveyMonkey was selected as the online survey vendor. The targeted population was 25,000 small to medium IT organizations with experienced IS managers, and security engineers that provided reliable assessments of the study variables at both the organizational and consumer levels.

The instrument, a *Self-Assessment Tool for Organizations*, measured the variables of this study. Using this instrument, six constructs were measured: (a) risk management, (b) physical security, (c) systems security, (d) network security, (e) wireless, and (f) data integrity and protection. Descriptive and inferential statistics were used. Appropriate measures were taken to ensure the ethical protection of the participants. The focus of Chapter 4 was the results of the study with a detailed discussion of the data collection and analysis process. Chapter 5 concludes the study with a detailed discussion of the results in relation to the reported literature. Additionally, recommendations for practice and future research are discussed.

Chapter 4: Results

Introduction

The purpose of this non-experimental quantitative study was to investigate and determine the security risk assessment practices IT administrators use to protect the confidentiality and integrity of the organization's information. I aimed to assess how IT managers of these organizations identify security threats associated with wireless networking, a major concern because of its relatively easy access (Kirankumar et al., 2012).

The following research questions and hypothesis statements of this study were constructed to investigate and assess the security practices by which IT administrators handle the security threats associated with wireless networking in the IT organization:

RQ1: What security risk assessments, if any, do IT administrators perform to protect the confidentiality and integrity of the organization's information?

H_01 : IT administrators do not regularly perform security risk assessments to protect the confidentiality and integrity of the organization's information.

H_a1 : IT administrators regularly perform security risk assessments to protect the confidentiality and integrity of the organization's information.

Research Question 2: Do network security risk management practices of IT administrators meet the minimally accepted practices and technical standards for wireless networking as measured by a security self-assessment survey?

H_{02} : The network security risk management practices of IT administrators do not meet the minimally accepted practices and technical standards for wireless networking as measured by a security self-assessment survey.

H_{a2} : The network security risk management practices of IT administrators do meet the minimally accepted practices and technical standards for wireless networking as measured by security self-assessment survey.

Chapter 4 is organized by following the headings: data collection, study results, and summary of findings.

Data Collection

Data were collected using the Securing Personal Information: A Self-Assessment Tool for Organizations instrument, with written permission from the authors. The six constructs measured were: (a) risk management, (b) physical security, (c) systems security, (d) network security, (e) wireless, and (f) data integrity and protection. Some of the questions on the original instrument were identified as minimum standards security requirements that all organization should meet or exceed. Questions shaded in blue on the survey indicated the minimum security requirements for any organization, regardless of its size or the sensitivity of the personal information it holds. The remaining questions help organizations raise their security standards beyond those minimum levels. The goal was for all IT participants to be able to answer “yes” to each question. However, to avoid response bias, I did not shade or reference minimum requirements on the survey in this study. All responses were tabulated in SPSS and coded as 1 = Yes, 2 = No. Other

questions represented additional levels of security that an organization may wish to consider when attempting to improve safeguarding personal and other sensitive data.

All data were collected via Internet using SurveyMonkey, an online commercial database. I uploaded an introductory letter explaining the purpose of the survey, a description of the role of the participant, explanation of how the data would be used, and an estimated time to complete the survey. Participants interested in the study were directed to the web-link to read the consent page. Participants were assured anonymity and therefore were not required to sign consent forms. Taking the survey implied consent.

On approval by Walden University's IRB (Approval Number 02-05-15-0129954), I sent more than 700 invitations to small and medium IT organizations ranging in sizes from 100-1,500 number of employees. Initially, only 25 individuals responded; therefore, I sent weekly reminders three times until I received 114 surveys. Data were then checked for missing items and incompletions. Of the 114 received, 113 were acceptable and complete. Raw data were then uploaded to Microsoft Excel spreadsheets for data analysis. The sampling selection was both random and convenient, which included members from both private and public organizations.

Data Analysis

In the present study, data analyses were conducted in three phases. First, I conducted a reliability test of the categorical responses (yes and no), followed by a series of descriptive analyses to compute the demographic variables. Although the authors previously validated the instrument, reliability testing is recommended when a different

population, in different settings is the target. The test for internal consistency of the items and reliability in the instrument was run in SPSS using Cronbach's alpha reliability test. The results showed an overall raw alpha of .955 for the 83 survey items, which is considered strong and acceptable. The cutoff value for being acceptable is reported to be .70 (Fink, 2013). The results are displayed in Table 5 that follows:

Table 6

Reliability Statistics

Reliability statistics		
Cronbach's alpha	Cronbach's alpha based on standardized items	N of Items
.954	.955	83

Second, a series of descriptive analyses were conducted which computed the demographic variables (see Table 6).

Table 7

Industry Type

	Frequency	percent	Valid percent	Cumulative percent
1 Public	35	30.7	31.0	31.0
2 Private	15	13.2	13.3	44.2
3 Government	48	42.1	42.5	86.7
4 Not for profit	15	13.2	13.3	100.0
Total	113	99.1	100.0	
Missing system	1	.9		
Total	114	100.0		

As shown in Table 6, the participants were 114 self-described IT personnel from various industries comprised of public (30.7%), private (13.2%), government (42.1%), and not for profit (13.2%). All were from organizations ranging in sizes from small to large with 35% reporting from organizations with 1500 or greater, 35% from organizations with 100-499, and the remainder between 500 or greater.

The frequency analysis for each of the six categories was summarized and reported as multiple responses in SPSS because of the large number of questions listed in each category (see Table 7). Overall, in every category participants responded “yes” greater than 79% of the time, an indication that most participants used generally accepted or common practices in each sector.

Table 8

Frequency Summary for All Categories

Categories	Responses	<i>N</i>	Percent
Risk management	Yes	92	81.3%
	No	22	18.7%
Physical security	Yes	90	79.4%
	No	24	20.6%
Security systems	Yes	94	82.6%
	No	20	17.4%
Wireless	Yes	96	84.1%
	No	18	15.9%
Data integrity	Yes	98	85.8%
	No	16	14.2%

As explained at the outset, some of the questions from each sector related to security requirements that an organization should, at minimum, meet or exceed. As shown in Table 3, all of the responses were tabulated according to the combined minimum and non-minimum categories. The data indicated that a majority (79%-86%) of the participants met the combined security requirements for managing security risks in the organization.

The means, standard deviation, and frequency count were computed in SPSS for the 83 survey items. The results indicated that the means and standard deviations were relatively similar for all variables ranging from high ($m = 1.51$, $SD .502$) to low ($m = 1.05$, $SD .228$) respectively. These findings indicated that the survey items were normally distributed (See Appendix B).

A one sample Chi-square test was conducted to determine whether a significant difference existed between the expected frequencies of the IT participants and the observed frequencies in the yes/no categories of each group of variables identified as minimum categories. To begin, I divided each data set into minimum categories. For the Risk Management category, 17 questions were listed. The author identified questions 1-6 and 8-14 as minimum *yes* responses. These questions were categorized as minimum. The results of the Chi-square test for this category were significant ($X^2 [1, n = 114] = 25.7-64.87$, $p < .001$). That is, because the Sig. value is .000 (see Table 8), which is less than .05, I can say there was a significant difference between the observed frequencies of the Risk Management minimum category and the expected values.

Table 9

Chi-Square Test Statistics

	Physical security	Systems security	Network security	Wireless	Data integrity	Risk management
Chi-square	60.193 ^a	49.782 ^b	30.364 ^c	74.028 ^c	56.467 ^d	64.877 ^e
<i>df</i>	1	1	1	1	1	1
Asymp. sig.	.000	.000	.000	.000	.000	.000

As shown in Table 8, the value labeled Asymp. Sig. (which is the *p*-value of the Chi-Square statistic) is .000 for all variables. The number of participants who responded *yes* ($n = 82$) was much greater than the number who responded *no*. The expected value was 52 and less. In every case, since the P-value (0.000) was less than the significance level (0.05), I rejected the null hypothesis. As a follow up test, I conducted a one-sample *t*-test for tests of the sample mean since the Chi square indicated a strong statistical difference between the categorical variables as indicated by the *yes* and *no* responses (see Table 9). The average of the sample (*M*) suggested that the participants came from a different population, which may have contributed to the significant differences reported in Chi square analysis.

Table 10

One Sample Test

Test Value = 0						
<i>t</i>	<i>df</i>	Sig. (2-tailed)	Mean difference	95% Confidence interval of the difference		
				Lower	Upper	
RM	36.365	113	.000	1.123	1.06	1.18
RM	36.365	113	.000	1.123	1.06	1.18
RM	34.293	113	.000	1.149	1.08	1.22
RM	37.257	113	.000	1.114	1.05	1.17
RM	31.371	112	.000	1.212	1.14	1.29
RM	32.135	113	.000	1.193	1.12	1.27
RM	31.437	111	.000	1.205	1.13	1.28
RM	33.055	112	.000	1.168	1.10	1.24
RM	31.561	107	.000	1.185	1.11	1.26
RM	32.390	109	.000	1.173	1.10	1.24
RM	32.168	108	.000	1.174	1.10	1.25
RM	31.990	109	.000	1.182	1.11	1.26
RM	30.028	105	.000	1.226	1.15	1.31
RM	29.896	108	.000	1.257	1.17	1.34
RM	31.118	108	.000	1.202	1.13	1.28
RM	31.118	108	.000	1.202	1.13	1.28
RM	29.520	108	.000	1.294	1.21	1.38

Study Results

The first research question asked, “What security risk assessments, if any, do IT administrators perform to protect the confidentiality and integrity of the organization’s information?” The null hypothesis stated, “Administrators do not regularly perform security risk assessments to protect the confidentiality and integrity of the organization’s information.” Two of the six survey constructs (questions 9 & 14) were used to assess

this question, Risk Management and Data Integrity and Protection. The overall results indicated that risk assessments were conducted at planned intervals to review the residual risks and the identified acceptable levels of risks. Overall, a large significant difference existed between the *yes* and *no* responses which indicated that an overwhelming majority of the IT administrators did regularly perform security risk assessments; therefore, the null hypothesis was rejected (See Table 10).

Table 11

Risk Management

Categories	Responses	<i>N</i>	Percent	Percent of cases
Risk management	Yes	92	81.3%	1346.5%
	No	22	18.7%	308.8%
Total		114	100.0%	1655.3%

In addition to assessing Risk Management reviews, I closely examined the variables of *Data Integrity and Protection* output returns (questions 77-83) to determine what percentage of participants met the minimum required responses of *yes*. This section was intended to be specific to securing the data from unauthorized modification. The results showed that overall 85% of the participants responded *yes* to questions related to data confidentiality and protection. More specifically, question 78 asked, if there was an archiving process that ensured the secure storage of data, and guarantees the continued confidentiality, integrity, and availability of the data. As displayed in Table 11, ninety-eight (92.5%) participants responded *yes*. For this reason, I concluded that IT

administrators regularly perform security risk assessments to protect the confidentiality and integrity of the organization's information; thereby, rejecting the null hypothesis.

Table 12

Data Integrity and Protection

Categories	Responses	<i>N</i>	Percent	Percent of cases
Data integrity	Yes	718	85.8%	677.4%
	No	119	14.2%	112.3%
Total		837	100.0%	789.6%

Research Question 2: Do network security risk management practices of IT administrators meet the minimally accepted practices and technical standards for wireless networking as measured by a security self-assessment survey? Two of the six constructs were used to assess this question, Network security (questions 54-60), and Wireless (questions 61-75). Computers, routers, and wireless access points make up the network security system, which transports and store technologies. Overall, 85.1% of participants responded yes to questions of network security.

Specifically, two items (62 and 63) required yes responses to meet the minimally accepted practices and technical standards. These were related to (a) the organization use of defense safeguards, such as firewalls and intrusion detection; and (b) servers supporting sensitive applications by removing unnecessary services and applications. Participants ($n = 102$) responded yes 94.4% and 86.1% respectively.

With regard to wireless assessment, a minimum of *yes* was required for survey questions (61 and 62): (a) Is there a policy in place that addresses the use of wireless technology? (b) Does the organization ensure that wireless networks are not used until they comply with the organization's security policy? Overall, 86.9 % to 91.6 % responded *yes*. The null hypothesis was rejected in favor of the alternative.

Summary

Chapter 4 provided the results of the descriptive and inferential statistics for the study population. The purpose of this non-experimental quantitative study was to investigate and determine the security risk assessment practices IT administrators use to protect the confidentiality and integrity of the organization's information. The data collection method for this study was a self-reported instrument using a cross-representation of industries and company sizes. Six constructs were used in the present study to address the research questions. (a) risk management, (b) physical security, (c) systems security, (d) network security, (e) wireless, and (f) data integrity and protection. The participants were 114 self-described IT administrators from organizations throughout the United States.

The analyses outcome in SPSS showed significant difference in participant responses to both research questions 1 and 2. The overall results indicated that an overwhelming majority (81.3%) of the IT administrators conducted risk assessments at planned intervals; therefore, I rejected the null hypothesis that stated, "Administrators do not regularly perform security risk assessments to protect the confidentiality and integrity of the organization's information." Additionally, the findings revealed that an

overwhelming majority (86.9%) of participants met or exceeded the minimally accepted practices and technical standards for wireless networking as measured by the security self-assessment survey. Therefore, I rejected the hypothesis for RQ2 that stated, “The network security risk management practices of IT administrators do not meet the minimally accepted practices and technical standards for wireless networking as measured by a security self-assessment survey. Chapter 5 concludes the study with a summary discussion of the findings, recommendations for future research, implications for positive social change, and conclusion.

Chapter 5: Summary, Conclusion, and Recommendations

Introduction

The purpose of this non-experimental quantitative study was to investigate and determine the security risk assessment practices IT administrators used to protect the confidentiality and integrity of each organization's information when using wireless networking. The participants were 114 men and women IT administrators from various organizations throughout the United States.

The central focus of the study was assessing the generally accepted or common practices of IT managers relevant to the relevance of a security safeguard. The self-assessment survey tool was used to assess the minimum-security requirements for any organization regardless of its size or the sensitivity of the personal information it held. The goal was for IT administrators to be able to answer "yes" to each question. The findings indicated that an overwhelming majority (89%) of participants answered yes to the survey questions in each sector of the survey. Chapter 5 summarizes the results of the study with respect to the following: interpretation of the findings, limitations of the study, recommendations, and conclusion.

Interpretation of Findings

The theoretical foundation for this study was based on a risk assessment and analysis framework, which was used for categorizing and sharing information about the risks and the necessary security safeguards needed for security management. Saleh et al. (2011) noted that a proper and efficient security risk assessment should result in

improved outcomes. The term *risk* was used in this study to describe the possible impact of threats to exposed and vulnerable information assets. Information assets were presented as values by using the properties of confidentiality, integrity, availability, and other properties essential to the organization.

The first research question asked, *What security risk assessments, if any, do IT administrators perform to protect the confidentiality and integrity of the organization's information?* Risk management was the first sector of the survey assessed, which focused on the actions of IT administrators when identifying the personal information assets of the organization. In addition, this sector assessed how organizations documented, analyzed, and evaluated the losses and damages resulting from personal information security invasions. The findings indicated that over 80% of IT administrators reported *yes* to analyzing, evaluating, and documenting information with respect to the personal impacts on customers and employees; possible threats and vulnerabilities; and the levels of acceptable risk.

A key component of risk management in the survey report was the risk review section. This sector examined the availability of a risk treatment plan that managed personal information security risks. More than 83% ($n = 94$) responded *yes* to this question. These findings suggested that more and more organizations are devising risk management plans to handle situations involving security related incidents such as hacking, copyright infringement, and defamation. It is crucial that organizations employ effective security methods for conducting IT risk assessment. For research question 1, I accepted the alternative hypothesis, which stated that IT administrators regularly perform

network security risk assessments to protect the confidentiality and integrity of the organization's information.

Chickowski (2013) noted that although security organizations may cover all of their bases in a routine IT risk assessment, such coverage should be carried out often enough to keep apprised of a growing number of new risks. The frequency with which IT administrators conduct the risk assessment process is almost as important as the means of carrying them out (Chickowski, 2013). Eighty-two percent (82%) of IT administrators reported they conducted risk assessments at planned intervals to review the residual and acceptable levels of risks, taking into account changes to the organization, technology, identified threats, and possible future threats.

The second research question examined the network security risk management practices of IT administrators relevant to meeting the minimally accepted practices and technical standards for wireless networking. Radack (2013) argued that maintaining secure wireless networks takes more frequent risk assessment and control evaluation than is required for other systems and networks. Overall, 83% of the IT administrators responded *yes* to the wireless sector of the survey. Over 90% claimed a policy was in place that addressed the use of wireless technology. These results were significant for wireless network security risk management (Tsai & Huang, 2011).

Other wireless actions reported by the IT administrators were confirmed as significant in the literature. For example, Radack (2013) argued that several steps should be taken by IT managers to achieve quality management of wireless systems. Radack believed that administrators should fully understand wireless network topology, conduct

frequent inventory on handheld and wireless devices, and back up data continually.

Additionally, they should periodically test and assess wireless network security, and track for standard changes in the wireless industry that would not only improve security, but also allow the release of new merchandise (Radack, 2013).

Consistent with Radack (2013), more than 82% of participants responded *yes* to having strong available security features enabled. However, only 70% said *yes* when asked whether the organization performed regular and random comprehensive security assessments, which included identifying unauthorized wireless access points and removing the devices. These findings suggested that the wireless networks of some organizations may be vulnerable and easy to attack. The literature indicated that wireless security is not solely a technical issue; a human factor is also present (Guo, Yuan, Archer, & Connelly, 2011; Kirankumar, Babu, Prasad, & Vishnumurthy, 2012). These factors must be addressed by appropriate countermeasures that involve employee awareness of the issues, user education, clearly stated organizational policies, and practices by management.

The self-assessment of physical security and system security responses were positive with a range of 85-92% responses for *yes*. Radack (2013) noted that physical controls should be implemented to protect wireless systems and information. Minimal physical security measures should include storing personal information in locked cabinets, locked office doors, pass cards, and intrusion alarm systems. The premise is that physical countermeasures can lessen risks such as theft of equipment and insertion of rogue access points or wireless network monitoring devices (Radack, 2013).

Security is just as critical and important in ad-hoc networks as in traditional networks. The sensitive data there should be protected from malicious eavesdroppers and network services should only be provided to eligible users (Butt, 2013). Taylor and Brice (2012) argued that too often when managers make security decisions, they do not have the requisite expertise regarding threats to their businesses' data. Consequently, they end up relying only on information readily available and a technology-based approach to addressing organization security risks. Taylor and Brice (2012) noted that most managers turn to trusted advisors such as IT managers to protect the organization from security breaches. The premise is that if management relies solely on this advice, the human element of organization security management may go unnoticed.

Toxen (2014) argued that a periodic security audit should be an ongoing process. Toxen believed that an outside security audit performed quarterly or annually and reviewed by senior management would have found the NSA's problems and, perhaps, fixed them in time to stop Edward Snowden who, while a contractor for the government NSA in Hawaii, copied and smuggled up to 1.7 million top-secret documents while working in the secured facility. These documents were leaked to the press and consequently altered the relationship of the United States government with other countries.

A key sector of the survey addressed the organization's policy relevant to the personal information stored on mobile and wireless devices. At minimum, all organizations should conduct a policy review and update policies at regularly scheduled intervals. The findings indicated that a majority (82%) of the participants responded yes

to having a policy in place for the organization. Written IT security policies are deemed necessary; however, organizations should have a way to check compliance (Aruba Networks, 2012). As such, many companies draft their own policies banning all wireless devices. However, since many users in the workplace demand mobility, users will install their own wireless connections or hotspots. These unauthorized access points effectively open an organization's network to intrusion by anyone in the neighborhood. Chenoweth et al. (2010) suggested that using a scanning technique would strengthen organizational policy. Users would be aware that they can be audited and would be more likely to remain compliant.

Most representatives in the study were aware that noncompliance put their information at a potential security risk. According to Meyer (2015), most corporations can honestly state they have a good set of security policies. However, where most companies fail is in executing these policies. This becomes a significant factor in data breaches. When a corporation has a data breach, the first question any external assessor, regulator or court official will ask is whether the proper policies were followed. If it was discovered, they were in noncompliance, that corporations will be viewed as negligent in its responsibilities. Therefore, it is essential for corporations to measure their policy compliances consistently. Implementing policies requires processes, procedures and standards that need to be established within the company, including ones for security breaches (Siponen, Mahmood, & Pahlila, 2009).

The last sector, *Data Integrity and Protection*, addressed procedures for securing employees removing authorized personal information from the premises. At minimal,

85% of the participants responded *yes* to this question. A security-related breach could cost an organization to lose personal information, resulting in a breach of confidentiality and integrity (Alshboul, 2010).

Aforementioned in the literature review, almost all established enterprises are targets, and the attacks have become more sophisticated as evidenced by the emergence of advanced persistent threats. Companies like Target, Sony's PlayStation Network, and many government agencies have firsthand knowledge the reputational and financial damage that occurs when private information is compromised or breached. The large retailer Target had its database breached in late 2013 and over 40 million customers had their personal information, stolen (Crosman, 2014). Sony's PlayStation Network was the victim of hackers accessing personal data for approximately 70 million Sony's PlayStation Network members. The information that was taken included addresses, credit card information, passwords, logins, and even security answers for the passwords (Yen, 2011). The Sony breach affected everyone, from executives to employees. Confidential information was leaked online and several Sony employees sued the company because of the breach. When news of the attack leaked, Sony's stock prices dropped dramatically. Another reminder, in South Carolina, the Department of Revenue reported two hackers breached the Department of Revenue's database and collected in excess of 3.5 million social security numbers and an additional 387,000 credit and debit cards (Zolkos, 2012).

Elkind (2015) described the recent breach security at Sony Pictures as the inside hack of the century. In November 2014, a devastating cyberattack was launched on Sony Pictures. Employees were met with menacing sounds, images and threats looming over

computer screens of personal computers and servers. Sony's IT staff immediately tried to pull the plug, but not before the hackers had wiped out everything stored on 3,262 of the company's 6,797 personal computers and 837 of its 1,555 servers. That was just the beginning of Sony's nightmare. Damages included dumping confidential files onto public file-sharing sites, destroying unfinished movie scripts, gaining access to emails, salary lists, and more than 47,000 Social Security numbers. The hackers threatened a 9/11-style attack against theaters, prompting Sony to abandon; "The Interview's Christmas" release. These are just a few examples of how security breaches in the corporate world can impact so many lives. Prakash and Singaravel (2014) described these type acts as information related terrorism; it means security violations and cyber terrorism through access control and other means.

As indicated in the literature review and as previously mentioned, so much personal and private information is now available electronically and on the web. These attacks on the databases, computers, networks, and the Internet can wreak havoc for businesses. Prakash and Singaravel (2014) argued that cyber terrorism could cause billions of dollars in damage to businesses if terrorists attack a company's information system and deplete accounts valuable accounts. Aforementioned, crippling a company's computer system means millions of dollars lost in productivity. It is therefore critical that the information systems be secure.

In summary, the security of data should be the main requirement of any IT organization. It is clear that in today's workplace, data sent and received in many electronic forms, expose companies to increased data hacks, threats, and losses (Kaur,

Rana, & Rishma, 2012). To minimize the security risk, organizations should perform security assessments before implementing wireless technologies to determine the specific threats and vulnerabilities that wireless networks are capable of producing in the organizational environments. Consideration for existing security policies, threats and vulnerabilities, company policies, safety issues, and costs for security measures are necessary (Spears & Barki, 2010). When the risk assessment is complete, the organization can begin planning and implementing the measures necessary to safeguard their systems and reduce their security risks to a manageable level. The policies and measures put in place should periodically be re-assessed because technologies and malicious threats are constantly changing (Xu, Hu, & Zhang, 2013).

Although the survey did not specifically address the level of employee training, education is important for many organizations. From a theoretical perspective, the way a user implements the various technologies, take the precautionary to protect the privacy of the organization is reflective of Bandura's (1982) theory. Bandura noted that behavior can be predicted by self-efficacy, perceived ease of use, and outcome judgments, how well an action can be executed by the individuals.

In the survey, many businesses answered that they did, in fact, have official strategies or processes for training employees on business' security policies.

It is essential, however, for IT managers to make sure employees make the right decision in their daily execution of their assigned tasks. For instance, employees know not to share passwords at workstations; however, an employee may find it simpler to just give his or her password to the next user, which can ultimately lead to vulnerabilities and potential

security breaches. That password can fall into the hands of someone who is less than honest. The key tenet is that it is not just about training employees but also making sure that they do the right thing to safeguard against a security breach.

In summary, security breaches are on the rise and as the number of information security incidents continues to escalate so do financial losses to the organization. A recent survey report in 2014 revealed the number of detected incidents costed 42.8 million dollars (PWC, 2015). It is a given fact that cyber risks will never completely be eliminated; however, organizations must remain vigilant and proactive in risk management and assessment in the face of a continually evolving vulnerabilities and threats.

Limitations of the Study

The limitations of the current study include the small sample size and the use of only six indicators assessing risk management. However, adding more than 83 questions could create response bias. Modifying some of these factors, such as survey length and the wording or items may help to decrease non-response for specific items. Per a shorter would insure that respondents are more likely to complete it. For IT managers, factors such as motivation, boredom, difficulty as well as time constraints could impact response time and completion.

Another limitation was geographical location. The survey was generated from IT industries within the Northeastern region of the United States of different sizes. Practices in larger organizations may differ for the smaller organization with fewer employees. As

a result, findings may not generalize to other organizations and businesses in regions throughout the United States.

Several limitations of this study can be addressed in future research. First, I believe that objective measures of security protection behaviors, though somewhat obtrusive in nature, should be considered. For instance, researchers could observe the workplace behavior of employees to obtain an assessment of the level of security compliance in the organization. Additionally, future studies could examine the behavior of employees before and after the implementation of new security training policies. The survey was tested in the United States, context and results might not be representative of the generalized global population. Therefore, the study could be replicated in other countries and in different organizational settings, and with larger sample groups for more generalizable findings. Additionally, further research is required for incorporating the identified key issues into information security management systems.

Recommendations

The results of this study set the stage for additional future research and recommendations. The key recommendations I suggest are literature based beginning with the theoretical concept of Risk Management. Although an overwhelming majority of participants indicated with *yes* responses that they conducted risk reviews on a regular basis, a substantial number had not (20-30%). More and more organizations should devise risk management plans to handle situations involving data integrity. It is crucial that organizations employ effective security methods for conducting IT risk assessment. With the rapid changing hacking climate, the frequency with which they conduct the risk

assessment process is almost as important as the means of carrying them out. The premise is that assessments should be carried out often enough to keep apprised of a growing number of new risks (Chickowski, 2013).

Radack (2013) described a whole range of actions or approaches that organizations can take to secure their devices and mobile networks, beginning with reviewing policies and understanding some of the associated risks. Most suggestions were related to mobile devices. A proper risk assessment should include a minimal of the following: (a) identifying the personal information assets of the organization and their sensitivities, (b) analyzing, evaluating and documenting the business losses or damages that might result from personal information security failures. This should include assessing the personal impact on the customers and employees and understanding the acceptable risks.

Business organizations rely heavily on Internet services to reduce cost and speed production. As such, regular reviews and risk assessments should be conducted at scheduled intervals to identify high levels of security risks. (Bojanc & Jerman-Blazic, 2013). Any penetration or threats may cause substantial loss for the company, subsequently stalling or shutting down business operations.

With regard to the wireless networking, Kirankumar, Babu, Prasad, and Vishnumurthy (2012) reported several ways to secure a wireless network from intruders. The most effective way was encryption or scrambling of communications over the network. Most wireless routers have built-in encryption mechanisms that can be turned off and on by the user. The second suggestion was to install anti-virus and anti-spyware

software and keeping them up-to-date. The third way was to turn off the mechanism called identifier broadcasting that sends out a signal to any device in the vicinity announcing its presence. This prevents hackers from honing in on vulnerable wireless networks (Kirankumar et al., 2012).

It is not possible to predict all areas of security risks needed for future research; however, in light of the findings and method used in the present research, I believe other methods would be suitable to explore the topic further. Future research using a qualitative approach is needed to gain an understanding of current issues in information security and IT management, together with an in-depth knowledge of a variety of techniques for strategically managing IT, both as a resource as well as for analyzing and controlling security risks.

C. Harrington (personal communication, 2015), Deputy Program Executive Officer of Health Service Systems, suggested the following:

The instrument may need updating to allow for additional responses to the questions such as do not know, not applicable, and written responses.

Additionally, since some questions concerning physical security may be out dated since technology has evolved to Common Access Cards (CAC). The CAC is a "smart" card about the size of a credit card used to enable physical access to buildings and controlled spaces, and it provides access to computer networks and systems. Many buildings are secured by CAC entry and departure (personal communication, June 15, 2015).

I believe that every IT administrator should be able to say *yes* to all of the survey questions. Obviously, this did not happen. Perhaps, a qualitative approach using a focus group would better capture the views of several participants. In addition, it would be a useful body of research to review the written policies of various organizations and compare what actually takes place with the written policy.

Implications

The overarching goal of this study is to strive for positive social change that impacts organizations and society in general. As part of a degree requirement Walden University defines positive social change as a deliberating process of creating and applying ideas and actions to promote the worth, dignity, and development of individuals, communities, organizations, institutions, cultures, and societies. Positive social change results in the improvement of human and social conditions. Information and communication technologies have been a key driving force in reshaping and improving our quality of life (Tiong, et al., 2006). It is a given fact that wireless technology initiatives provide greater opportunities for social impact than many other information and communications technologies. For example, physical access to mobile phones, tablets, and laptops is obviously more prevalent compared to computers and other less readily available technologies. Many organizations are installing and implementing wireless networks.

With the widespread growing mobile network coverage and use of mobile and handheld devices, obviously come security risk that can impact lives forever. Outside intruders can connect to wireless access points. Internet connections used by employees

to download music, games, and other applications, reduce employee productivity and place the company at risk for unauthorized users to use the Internet connection for malicious purposes such as hacking. By using the Internet line, intruders often conceal themselves under protective cover and appear to be a part of your business. Businesses are at risk if the intruder is doing illegal activity, such as collecting and distributing private information. This was demonstrated in the recent security breach at Sony Pictures with the inside work described as the hack of the century (Elkind, 2015).

In recent weeks, a reporter for the Washington Post reported that China hacked into the federal government's network, compromising four million current and former employees' information (Nakashima, 2015). The hack was the largest breach of federal employee data in recent years. It was the second major intrusion of the same agency by China in less than a year and the second significant foreign breach into United States government networks in recent months. Last year, Russia compromised White House and State Department e-mail systems in a campaign of cyberespionage. When these types of activities occur into restricted government networks, the government image and reputation are at stake. Organizations are largely responsible for any and all activities related to the Internet connection.

Based on the recent turn of events of breach in the literature and news media, the implications of this study for the practice of Systems' Information Management and other related disciplines are unlimited. With wireless and mobility permeating in organizations and society in general, now is a good time for IT administrators to review the risks, security policies, and protection that are in place in their various organizations.

The recent events clearly validate the literature reviewed, which provided evidence that wired networks compared with wireless networks might be more vulnerable and easy to attack (Kirankumar et al., 2012). In a wired network, hackers or attackers gain access by penetrating some physical security perimeter to gain network access, whereas, in wireless networking, attackers easily gain access without getting into a building or physical setting. However, the literature indicated that wireless security is not solely a technical issue, a human factor is also present (Guo, Yuan, Archer, & Connelly, 2011). These factors must be addressed by appropriate countermeasures that involve employee awareness of the issues, user education, clearly stated organizational policies, and practices by management.

Taylor and Brice (2012) argued that too often when managers make security decisions, they do not always have the requisite expertise regarding threats to their businesses' data. Consequently, they end up relying on only information readily available and a technology-based approach to addressing organization security risks. Taylor and Brice (2012) noted that most managers turn to trusted advisors, whom they consider experts, to protect the organization from security breaches (example, the Information Technology (IT) manager). The premise is that if management relies solely on this advice, the human element of organization security management may go unnoticed.

As the findings indicated, most companies have policies for wireless and mobility in place. Reviewing policies will send a clear message to the business and users that administrators are serious about wireless and mobile security. It is important to note that many of the security threats have changed and migrated down from enterprises to smaller

businesses. However, as the findings indicated, many organizations (20% or greater) have not reviewed their wireless and mobility risks in line with increasing wireless use.

The literature reviewed makes it clear that regardless of what countermeasures are applied, it is not practical or possible to defend any organization or business against all of the many possible attacks; suggesting that a more realistic goal is to reduce the associated risk to a more acceptable level (Phifer, 2008). Aforementioned, a good first step is to begin by identifying one's own wireless vulnerabilities and possible attackers. With this in mind, an organizational IT manager should follow several steps considered necessary in performing risk analysis recommended by Phifer (2008). They were the following: (a) define the business needs of the organization; (b) identify and certify who needs wireless networking access and where; (c) carefully classify individuals or departments who are allowed to use 802.11 in the workplace and mobile devices off site; and (d) regulate which applications and databases should be accessible to wireless users (Phifer, 2008; Radack, 2013).

Aside from these key steps, the IT manager needs to regularly assess and quantify any new risks to the business caused by adding wireless networking. That is, managers should estimate the potential cost to business during downtime and recovery expenses. This positions the manager to be able to write and implement enforceable security policies (Radack, 2013). Phifer (2008) argued that to be truly effective, managers should carry out regular assessments to spot new vulnerabilities and to verify that installed security measures are working as intended. These assessments may be performed internally or by third-party individuals who are knowledgeable or have no knowledge of

the organization's security networks. The premise is that organizations and individuals reap benefit when wireless networks and devices are protected from deliberate and intentional threats. Again, it is important to stress that although no perfect system exists that can prevent all penetrations; countermeasures can offer some managerial solutions to reduce many common risks associated with wireless technology.

The IT organizations in this study ranged in sizes from small to medium with 100-1500 number of employees. Meyer (2015) argued that regardless of organizational size or regulatory requirement, companies should establish a risk committee that has oversight of business resilience risks and make cyber threats and vulnerabilities a focal pillar of the risk management program reporting to the board. Having a business resilience plan that includes cyber will not only save money on impacting events, but will also allow business to resume much more quickly than if data are lost or compromised.

All corporations are subject to the risk of a data security breach. While it can be a gut-wrenching ordeal, known how to manage a breach can make it much easier to contain the damage. Although, the survey did not specifically address the training aspects of IT employees, the findings clearly indicated that training is needed for all employees and managers to ensure at a minimum, they are aware of and understand their security responsibilities, as well as their security policies and practices. This should include understanding permitted access, and use and disclosure of personal information.

Risk management involves a number of human activities which are based on the way the various stakeholders perceive risk associated with IS assets. I believe that both organizations and individuals can greatly benefit when security measures are properly

addressed to protect the wireless networks and wireless devices used for business applications. When IT managers properly and frequently assess the risks associated with wireless technologies in their companies, they can effectively reduce the risks by taking early actions to address specific threats and vulnerabilities. While this study may not prevent all penetrations and adverse events in the organization, it can be effective in bringing attention to how IT managers can reduce many of the common risks associated with wireless computing.

Additionally, this study is able to contribute to theory and practice. Results of the study demonstrated support for the IT management perspective and thus provided a valid framework in studying employee security behavior in the organization. When the results of the study are published, industry experts will gain insight on how employee behaviors is relevant to security guidelines can be addressed and managed effectively.

Conclusions

Security risk in wireless networks is one of the major problems facing wireless IT organizations today. The findings from the study demonstrated that with the rapid rise of wireless technology in organizations, risk management is necessary to secure the information and assets of the company. IT managers from all sizes and types of organizations used measures to reduce the risks by applying the appropriate actions to counter the specific threats. Also, security risk assessments can aid in the implementation of security policies and guidelines. While, not all measures will prevent all possible invasions and threats, researchers confirmed they can be effective in reducing many of the risks associated with wireless technology.

References

- Abiona, O., Oluwaranti, O. Oluwatope, A., Bello, S., Onine, C. Sanni, M. & Kehinde, L. (2013). Wireless network security: The mobile agent approach. *Int. J. Communications, Network and System Sciences*, 2013, 6, 443-450.
<http://dx.doi.org/10.4236/ijcns.2013.610046>
- Aldhizer, G. I. (2008). The insider threat. *Internal Auditor*, 65(2), 71-73. (Accession No. 510784119)
- Alshboul, A. (2010). Information systems security measures and countermeasures: Protecting organizational assets from malicious attacks. *Communications of the IBIMA*. Retrieved from <http://www.ibimapublishing.com/journals/CIBIMA/2010/486878/486878.pdf>
- The American Legion. (2014). *VA's eBenefits suffers data breach*. Retrieved from <http://www.legion.org/veteransbenefits/218278/vas-ebenefits-suffers-data-breach>
- Ammari, N., Ghallali, M., El Kalam, A. A., El Hami, N., Ouahman, A. A., & El Ouahidi, B. (2014). Mobile security: Security mechanisms and protection of mobile applications. *Journal of Theoretical & Applied Information Technology*, 70(2), 302-315. doi:10.1145/2184319.2184330
- Ansilla J., D., Vasudevan, N., & Ravi, S. (2015). Enhancing data security to handle DoS and SYN flood attack with hardware implementation. *Journal of Theoretical & Applied Information Technology*, 71(3), 396-405. (Accession No.100755412)

- Aruba Networks. (2012). Building global security policy for wireless LANs. Retrieved from http://www.arubanetworks.com/pdf/technology/whitepapers/wp_Global_security.pdf
- Ayyagari, R. (2012). An exploratory analysis of data breaches from 2005-2011: Trends and insights. *Journal of Information Privacy & Security*, 8(2), 33-56. (Accession No. 80511757)
- Bandura, A. (1982), Self-efficacy mechanism in human agency, *American Psychologist* 37(2) 122-147. Retrieved from <http://www.uky.edu/~eushe2/Bandura/Bandura1982AP.pdf>
- Berghel, H., & Uecker, J. (2005). WiFi attack vectors. *Communications of the ACM*, 48(8), 21-28. (Accession No. 510784119)
- Bischoff, H., Sinay, J., & Vargová, S. (2014). Integrated risk management in industries from the standpoint of safety and security. *Transactions of the VSB - Technical University Of Ostrava, Safety Engineering Series*, 9(2), 1-7. (Accession No. 102604833).
- Bojanc, R., & Jerman-Blazic, B. (2013). A quantitative model for information-security risk management. *Engineering Management Journal*, 25(2), 25-37. Retrieved from <http://search.proquest.com/docview/1434438214?>
- Borrett, M., Carter, R., & Wespi, A. (2013). How is cyber threat evolving and what do organizations need to consider? *Journal of Business Continuity & Emergency Planning*, 7(2), 163-171.

- Butt, S. (2013). A survey of security approaches for wireless AD-HOC networks. *Golden Research Thoughts*, 2(9), 1-10. (Accession No. 510784119)
- Cereola, S. J., Wier, B., & Norman, C. (2012). Impact of top management team on firm performance in small and medium-sized enterprises: Adopting Commercial Open-Source Enterprise Resource Planning. *Behaviour & Information Technology*, 31(9), 889-907. doi:10.1145/2184319.2184330
- Chenoweth, T., Minch, R., & Tabor, S. (2010). Wireless insecurity: Examining user security behavior on public networks. *Communications of the ACM*, 53(2), 134-138. (Accession No. 102604833)
- Chickowski, E. (2013). Once-a-year risk assessments aren't enough. Retrieved from <http://www.darkreading.com/risk/once-a-year-risk-assessments-arent-enough/240163427>
- Choi, N., Kim, D., Goo, J., & Whitmore, A. (2008). Knowing is doing. *Information Management & Computer Security*, 16(5), 484-501.
<http://dx.doi.org/10.1108/09685220810920558>
- Cox, J. (2010). Best enterprise wireless secrets revealed. *Networkworld Asia*, 6(1), 20-22.
doi:10.1109/TR.2011.2170117
- Creswell, J. W. (2009). *Research design: Qualitative, quantitative, and mixed methods approaches* (3rd ed.). Thousand Oaks, CA: Sage Publications, Inc.

- Crosman, P. (2014, Jan 23). Cheat sheet: What bankers need to know about the target breach. *American Banker*. Dance, S. (2014, March 14). UM data breach slightly smaller than thought. *The Baltimore Sun*. Retrieved from <http://www.baltimoresun.com/business/technology/blog/bs-md-umd-data-breach-update-20140312,0,1173810>
- Davis, F. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, *13*, 319-340.
- Defense Acquisition University (2014). Automated information systems. Retrieved from <https://dap.dau.mil/gateways/ma/Pages/InformationTechnology.aspx>
- Dhull, S., & Singh, J. (2010). Study of vulnerabilities in wireless local area networks (WLAN). *International Journal of Educational Administration*, *2*(3), 727-731. doi:10.1109/TR.2011.2170115
- Dong, L. Zhe, G., Baoyu, A Yangxi, O., Wei, C., & Hongliang, Z. (2012). A novel security management scheme in wireless sensor networks. *International Journal of Advancements in Computing Technology*, *4*(10), 36-44. Retrieved from Ebsco database.
- Elkind, P. (2015). Inside the hack of the century. *Fortune*, *172*(1), 64-89. Accession No. 502039390
- Farahmand, F., Navathe, S. B., Sharp, G. P., & Enslow, P. H. (2005). A management perspective on risk of security threats to information systems. *Information Technology and Management*, *6*(2-3), 203-225. doi:10.1145/2184319.2184330

- Faul, F., Erdfelder, E., Buchner, A., & Lang, A. G., (2007) Statistical power analyses using G*Power 3.1: Tests for correlation and regression analyses. Retrieved from http://www.gpower.hhu.de/fileadmin/redaktion/Fakultaeten/Mathematisch-Naturwissenschaftliche_Fakultaet/Psychologie/AAP/gpower/GPower31-BRM-Paper.pdf
- Fenz, S., Ekelhart, A., & Neubauer, T. (2011). Information security risk management: In which security solutions is it worth investing? *Communications of the Association for Information Systems*, 28(1), 329-356. . doi:10.1007/s10799-005-5880-5
- Fink, A. (2013). *How to conduct surveys. A step by step guide* (5th ed.). London, UK. Sage
- Fishbein, M. & Ajzen, I. (1975). *Belief, attitude, intention, and behavior: An introduction to theory and research*. Reading, MA: Addison-Wesley.
- Friesen, M. R. and McLeod, R. D. (2014) Smartphone Trajectories as Data Sources for Agent-Based Infection-Spread Modeling, in *Analyzing and Modeling Spatial and Temporal Dynamics of Infectious Diseases* (eds D. Chen, B. Moulin and J. Wu), John Wiley & Sons, Inc., Hoboken, NJ, USA. doi: 10.1002/9781118630013.ch20
- Garfinkel, S. (2012). The cybersecurity risk. *Communications of the ACM*, 55(6), 29-32. doi:10.1145/2184319.2184330
- Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Richardson, R. (2005). CSI/FBI computer crime and security survey, Computer Security Institute. Retrieved from: <http://www.cpppe.umd.edu/Bookstore/Documents/2005CSISurvey.pdf>.
- Greengard, S. (2013). Human and system errors lead to data breaches. *Baseline* 2.

- Gregor, U., & Krone, T. (2006). Mobile and wireless technologies: Security and risk factors. *Trends & Issues in Crime & Criminal Justice*. Retrieved from http://www.aic.gov.au/media_library/publications/tandi_pdf/tandi329.pdf
- Guo, K. H., Yuan, Y., Archer, N. P., & Connelly, C. E. (2011). Understanding Nonmalicious Security Violations in the Workplace: A Composite Behavior Model. *Journal Of Management Information Systems*, 28(2), 203-236. . doi:10.1109/TR.2011.2170117
- Hu, Q., Xu, Z., & Dinev, T. (2011). Does deterrence work in reducing information security policy abuse by employees? *Communications of the ACM*, 54(6), 54-60. Accession No. 502039390
- Hyeokchan, K., & Sin-Hyo, K. (2013). Improving mobile device classification using security events for preventing wireless intrusion. *International Journal of Security & Its Applications*, 7(6), 181-190. doi:10.14257/ijisia.2013.7.6.19
- ISACA.org (2009-2014). An introduction to the business model for information security. Retrieved from <http://www.isaca.org/Knowledge-Center/BMIS/Documents/IntrotoBMIS.pdf>
- Jones, C. M., McCarthy, R. V., & Halawi, L. (2010). Utilizing the technology acceptance model to assess the employee adoption of information systems security measures. *Journal of International Technology and Information Management*, 19(2), 43-II. Retrieved from <http://search.proquest.com/docview/847661664?>

- Jourdan, Z., Rainer, R. K., Marshall, T. E., & Ford, F. N. (2010). An investigation of organizational information security risk analysis. *Journal of Service Science*, 3(2), 33-42. Retrieved from <http://search.proquest.com/docview/822992687?>
- Kassar, M., Kervella, B., & Pujolle, G., (2008). An overview of vertical handover decision strategies in heterogeneous wireless networks. *Computer Communications*, 31(10), 2607–2620. doi:10.1145/2184319.2184330
- Kim, P. S. (2013). An alternative IEEE 802.21-assisted PMIPv6 to reduce handover latency and signaling cost. *Engineering Letters*, 21(2), 68-71. (Accession No. 102604833).
- Kirankumar, B., Babu, V. M., Prasad, D. S., & Vishnumurthy, R. (2012). Wireless security system. *International Journal of Computer Science and Information Security*, 10(4), 140-144. Retrieved from <http://search.proquest.com/docview/1038461385?>
- Kaur, M., Rana, P., & Rishma (2012). Database security in wireless sensor network through PGP and ID3. *International Journal of Engineering Science and Technology*. 4(6). ISSN : 0975-5462
- Kumar, R. L., Park, S., & Subramaniam, C. (2008). Understanding the value of countermeasures portfolios in information systems security. *Journal on Management Information Systems*, 25, 241-279. doi:10.1145/2184319.2184330

- Kwo-Shing Hong, Yen-Ping, C., Chao, L. R., & Tang, J. (2003). An integrated system theory of information security management. *Information Management & Computer Security*, 11(5), 243-248. Retrieved from <http://search.proquest.com/docview/212366703?accountid=35812>
- Lampson, B. (2009). Privacy and security: Usable security: How to get it. *Communications of the ACM*, 52(11), 25-27. doi:10.1177/0021943612465181
- Liao, K., & Chueh, H. (2012). Medical Organization Information Security Management Based on ISO27001 Information Security Standard. *Journal Of Software* (1796217X), 7(4), 792-797. doi:10.4304/jsw.7.4.792-797
- Lalitha, T., Kumar, S., & Hamsaveni, R. (2014). Efficient key management and authentication scheme for wireless sensor networks. *American Journal of Applied Sciences*. 11(6).969-977. DOI : 10.3844/ajassp.2014.969.977
- Likhar, P., Yadav, R., & Rao M., K. (2011). Securing IEEE 802.11g Wlan using open VPN and its impact analysis. *International Journal of Network Security & Its Applications*, 3(6), 97-113. doi:10.5121/ijnsa.2011.3607
- Liu, L., Stimpson, T., Antonopoulos, N., Ding, Z., & Zhan, Y. (2014). An Investigation of Security Trends in Personal Wireless Networks. *Wireless Personal Communication*. 75(3). 1669-1687. Doi:10.1007/s11277-013-1386-3
- Loo, A. (2008). The myths and truths of wireless security. *Communications of the ACM*, 51(2), 66-71. . doi:10.1007/s10799-005-5880-5
- Loo, A. W. (2010). Illusion of wireless security. *Advances in Computers*, 79, 119-167.

- Maheshwari, H. K., & Kemp, A. H. (2012). Performance analysis of ranging with IEEE 802.15.4 Compliant WSN Devices. *Ad-hoc & Sensor Wireless Networks*, 15(2-4), 223-254. doi:10.1177/0021943612465181
- Manikandan, C. C., Parameshwaran, R. R., Hariharan, K. K., Kalaimani, N. N., & Sridhar, K. P. (2013). Combined security and integrity agent integration into NS-2 for wired, wireless and sensor networks. *Australian Journal of Basic & Applied Sciences*, 7, 376-382. doi:10.1177/0021943612465181
- Maqousi, A., Balikhina, T., & Mackay, M. (2013). An effective method for information security awareness raising initiatives. *International Journal of Computer Science & Information Technology*, 5(2), 63-72. doi:10.5121/ijcsit.2013.5206
- Mashhour, A. S., & Saleh, Z. (2013). Wireless networks security in Jordan: A field study. *International Journal of Network Security & Its Applications*, 5(4), 43-52. doi:10.5121/ijnsa.2013.5403
- McCafferty, D. (2010). Security slideshow: Ernst & Young information security report card, *CIO Insight*. Retrieved from <http://www.cioinsight.com/c/a/Security/Ernst-Young-Information-Security-Report-Card-374955/>
- Mohamad, R. Zakaria, & Nabil, Zulhemay, M. (2013). The relationship of information security knowledge (risk) and human factors: challenges and solution. *Journal of Theoretical & Applied Information Technology*, 57(1), 67-75. (Accession No. 102604833).

- Moorthy, M., & Sathiyabama, S. (2012). Effective authentication technique for distributed denial of service attacks in wireless local area networks. *Journal of Computer Science*, 8, 828-834. Retrieved from <http://search.proquest.com/docview/1081878349?>
- Meyer, A. (2015). Lessons from the Sony breach in risk management and business resiliency. *Network World*. Retrieved from <http://www.networkworld.com/article/2867313/network-security/lessons-from-the-sony-breach-in-risk-management-and-business-resiliency.html>
- Nakashima, E. (2015). Chinese breach data of 4 million federal workers. *Washington Post*. Retrieved from https://www.washingtonpost.com/world/national-security/chinese-hackers-breach-federal-governments-personnel-office/2015/06/04/889c0e52-0af7-11e5-95fd-d580f1c5d44e_story.html
- Office of the Information and Privacy Commissioner for British Columbia (2012). *Securing Personal Information: A Self-Assessment Tool for Organizations*. Retrieved from: <https://www.oipc.bc.ca/guidance-documents/1439>
- OPC Privacy Policy (2012). Noncommercial Reproduction. Retrieved from http://www.priv.gc.ca/notice-avis_e.asp#004
- Pandey, S. (2011). Modern network security: Issues and challenges. *International Journal of Engineering Science & Technology*, 3, 4351-4357. doi:10.1145/2184319.2184330

- Pazos, P., Chung, J. M., & Micari, M. (2013). Instant messaging as a task-support tool in information technology organizations. *Journal of Business Communication*, 50(1), 68-86. doi:10.1177/0021943612465181
- Phifer, L. (2008). WLAN security: Best practices for wireless network security. Retrieved from: <http://searchsecurity.techtarget.com/WLAN-security-Best-practices-for-wireless-network-security>.
- Prakash, M. & Singaravel, G. (2014). An analysis of privacy risks and design principles for developing countermeasures in Privacy preserving sensitive data publishing. *Journal of Theoretical and Applied Information Technology*. 62(1). 204-213. ISSN: 1992-8645
- Privacy Rights Clearinghouse (2011). Empowering consumers. Protecting privacy. Retrieved from <https://www.privacyrights.org/category/year/2011>
- PWC (2015). Global state of information security: 2015. Retrieved from: <http://www.pwc.com/gx/en/consulting-services/information-security-survey/index.jhtml>
- Radack, S. (2013) Security for wireless networks and devices. Computer Security Division, National Institute of Standards and Technology. Retrieved from <http://www.itl.nist.gov/lab/bulletns/bltnmar03.htm>
- Ramos, A., & Holanda Filho, R. (2015). Sensor Data Security Level Estimation Scheme for Wireless Sensor Networks. *Sensors* (14248220), 15(1), 2104-2136. doi:10.3390/s150102104

- Research Information Ltd. (2011a). Data breaches cost the healthcare industry an estimated \$6.5 billion. (2011). *International Journal of Micrographics & Optical Technology*, 29(3), 3-4. doi:10.1145/2184319.2184330
- Research Information Ltd. (2011b). Best practices for disaster preparedness of business records. *International Journal of Micrographics & Optical Technology*, 29(3), 5. (Accession No. 102604833).
- Rhodes, K., & Kunis, B. (2011). Walking the wire in the wireless world: legal and policy implications of mobile computing. *Journal of Technology Law & Policy*, 16(1), 25-52. doi:10.1109/TR.2011.2170117
- Roobahani, F. S., & Azad, R. (2015). Security Solutions against Computer Networks Threats. *International Journal Of Advanced Networking & Applications*, 7(1), 2576-2581. Accession Number: 109051903
- Sabnis, S., Verbruggen, M., Hickey, J., & McBride, A. J. (2012). Intrinsically Secure Next-Generation Networks. *Bell Labs Technical Journal*, 17(3), 17-36. doi:10.1002/bltj.21556
- Saleh, Z. I., Refai, H., & Mashhour, A. (2011). Proposed framework for security risk assessment. *Journal of Information Security*, 2(2), 85-90. Retrieved from <http://search.proquest.com/docview/866646563?>
- Scherer, M., & Shuster, S. (2013). Number two Edward Snowden the dark prophet. *Time International*, 182(26), 78. (Accession number 93341345)
- Shipley, G. (2010). Epic fail. *InformationWeek*, (1282), 26-38. Retrieved from <http://search.proquest.com/docview/760099644?>

SECNAP Network Security (2012). Network vulnerability assessments and scans.

Retrieved from: <http://www.secnap.com/support/faqs/network-vulnerability-assessments.html>

Singh, R., & Sharma, T. (2014). A Key Hiding Communication Scheme for Enhancing the Wireless LAN Security. *Wireless Personal Communications*, 77(2), 1145-1165. doi:10.1007/s11277-013-1559-0

Siponen, M., Mahmood, M., & Pahlila, S. (2009). Are employees putting your company at risk by not following information security policies? *Communications of the ACM*, 52(12), 145-147. doi:10.1002/bltj.21556

Sivaprasatham, V. & Venkateswaran, J. (2012). A secure key management technique for wireless body area networks. *Journal of Computer Science* 8 (11), 1780-1787, doi:10.3844/jcssp.2012.1780.1787

Spears, J. L., & Barki, H. (2010). User participation in information systems security risk management. *MAIS Quarterly*, 34, 503-522. Retrieved from: <http://aisel.aisnet.org/cgi/viewcontent.cgi?article=2918&context=misq>

Taylor, R. G., & Brice, J., Jr. (2012). Fact or fiction? A study of managerial perceptions applied to an analysis of organizational security risk. *Journal of Organizational Culture, Communication and Conflict*, 16(1), 1-23. Retrieved from <http://search.proquest.com/docview/1037691839?>

Teer, F. P., Kruck, S. E., & Kruck, G. P. (2007). Empirical study of students' computer security practices/perceptions. *The Journal of Computer Information Systems*, 47(3), 105-110. Retrieved from <http://search.proquest.com/docview/232583860?>

- Thangavel, M., & Thangaraj, P. (2011). Efficient hybrid network (wired and wireless) intrusion detection using statistical data streams and detection of clustered alerts. *Journal of Computer Science*, 7(9), 1318-1324. doi:10.1002/bltj.21556
- Tharp, T. (2008) Assessing IT risks in the health-care industry. Retrieved from <https://iaonline.theiia.org/assessing-it-risks-in-the-health-care-industry>
- Tiong, I. C., Hafeez-Baig, A., Gururajan, R., & Soar, J. (2006). Preliminary investigation to explore perceptions of security issues associated with wireless technology in healthcare in Australia. In: Westbrook, J. and Callen, J., (ed.). HIC 2006 Bridging the Digital Divide: Clinician, consumer and computer, Health Informatics Society of Australia Ltd. (HIC 2006, 20-22
- Toxen, B. (2014). The NSA and Snowden: Securing the All-Seeing Eye. *Communications of the ACM* 57(5). 44-49. doi: 10.1145/2594502
- Trochim, W., & Donnelly, P. (2008). *The research methods knowledge base* (3rd ed.). Cincinnati, OH: Atomic Dog.
- Tsai, H., & Huang, Y. (2011). An analytic hierarchy process-based risk assessment method for wireless networks. *IEEE Transactions On Reliability*, 60(4), 801-816. doi:10.1109/TR.2011.2170117
- USA Today (2014). Russian data breach coincides with security conference. Retrieved from <http://www.usatoday.com/story/tech/2014/08/06/russian-crime-ring-cybersecurity/13658595/>

- United States CERT (2014). Retrieved from <http://www.us-cert.gov/publications/securing-your-web-browser>
- Venkataraman, S., Brumley, D., Sen, S., & Spatscheck, O. (2013). Automatically inferring the evolution of malicious activity on the internet. Retrieved from <http://www.internetsociety.org/doc/automatically-inferring-evolution-malicious-activity-internet>
- Vakil, F. (2005). Wireless networks and security issues. *Review of Business*, 26(3), 10-12. doi:10.1002/bltj.21770.
- Vanitha, M. M., Selvakumar, R. R., & Subha, S. S. (2013). Hardware and software implementation for highly secured modified wired equivalent privacy (Mdwp). *Journal of Theoretical & Applied Information Technology*, 48(2), 668-673. doi:10.1002/bltj.21556
- Wall, V. (2013). Greenwald on Snowden leaks: The worst is yet to come. Retrieved from <http://world.time.com/2013/10/14/greenwald-on-snowden-leaks-the-worst-is-yet-to-come/>
- Warner, J. (2011). Experiencing IT security in an organizational environment: Conceptualization and measurement development of an individual level IT security climate construct. *The Business Review, Cambridge*, 18(2), 67-74. Retrieved from <http://search.proquest.com/docview/925638755?>

- WatchGuard Technologies. (2013, Oct 8). WatchGuard technologies brings big data visibility tools to network security; zero-install, cloud-ready WatchGuard dimension instantly distils 'oceans of security data' into key insights and trends. (2013, Oct 08). *M2 Presswire*. Retrieved from <http://search.proquest.com/docview/1440066848?>
- Weisbrot, M. (2013). Comment: We can help Snowden: The NSA whistle blower has been offered asylum, but he still needs citizens' support to achieve it. *The Guardian*, p. 26. Retrieved from <http://search.proquest.com/docview/1373216743?>
- Wilkie, L., & Mensch, S. (2012). Wireless computing technology. *Global Education Journal*, 2012(3), 1-36. doi:10.1002/bltj.21556
- Xiong, N., Yang, F., Li, H., Park, J., Dai, Y., & Pan, Y. (2011). Security analysis and improvements of IEEE standard 802.16 in next generation wireless metropolitan access network. *Wireless Communications & Mobile Computing*, 11(2), 163-175. doi:10.1002/wcm.872
- Xu, Z., Hu, Q., and Zhang, C., (2013). Why computer talents become computer hackers. *Communications of the ACM*, 56(4), 64-74. doi:10.1002/bltj.21556
- Yen, A. (2011, April 26). Sony confirms massive PlayStation Network breach—What you should know. Retrieved from <http://lalawag.com/2011/04/26/sony-confirms-massive-playstation-network-breach-what-you-should-know/>

- Yu, G., & Weng, K. (2013). The throughput for multi-hop relay wireless sensor networks based on cooperative diversity. *Journal of theoretical & applied information technology*, 52(1), 1-10 . Accession Number: 89673032
- Zolkos, R. (2012). S.C. data breach highlights public entity risks. *Business Insurance*, 46(43), 1. Retrieved from <http://www.businessinsurance.com/article/20121104/NEWS06/311049983>

Appendix A: Wireless Questions from Security Self-Assessment Tool

4 Human Resources Security

Executive Leadership

- 4.1 Does management actively support personal information security within the organization through clear direction, demonstrated commitment, explicit assignment, and acknowledgment of personal information security responsibilities? YES NO
- 4.2 Is there a management-level employee (and management-level contractor representative, where a contract is in place) identified as responsible for security practices? YES NO
- 4.3 Is there a functional forum of management representatives from IT and business units to coordinate and implement personal information security controls? YES NO

Training

Has training been implemented for all employees, data custodians and management to ensure they are aware of and understand:

- 4.4 Their security responsibilities? YES NO
- 4.5 Security policies and practices? YES NO
- 4.6 Permitted access, use and disclosure of personal information? YES NO
- 4.7 Retention and disposal policies? YES NO
- 4.8 Requirements for password maintenance and proper password security? YES NO
- 4.9 Is annual privacy and security training a requirement for any handling of personal information? YES NO
- 4.10 Are there consequences, such as blocking access to personal information, if employees do not complete annual privacy and security training? YES NO
- 4.11 Are there consequences for compromising keys, passwords and other security policy violations? YES NO
- 4.12 Is completion of privacy and security training tracked? YES NO

Blue text indicates a minimum security requirement. 

Appendix B: Descriptive Statistics

Risk Management (RM)

	N	Mean	Std. Deviation	Minimum	Maximum	Percentiles		
						25th	50th (Median)	75th
RM	114	1.12	.330	1	2	1.00	1.00	1.00
RM	114	1.12	.330	1	2	1.00	1.00	1.00
RM	114	1.15	.358	1	2	1.00	1.00	1.00
RM	114	1.11	.319	1	2	1.00	1.00	1.00
RM	113	1.21	.411	1	2	1.00	1.00	1.00
RM	114	1.19	.396	1	2	1.00	1.00	1.00
RM	112	1.21	.406	1	2	1.00	1.00	1.00
RM	113	1.17	.376	1	2	1.00	1.00	1.00
RM	108	1.19	.390	1	2	1.00	1.00	1.00
RM	110	1.17	.380	1	2	1.00	1.00	1.00
RM	109	1.17	.381	1	2	1.00	1.00	1.00
RM	110	1.18	.387	1	2	1.00	1.00	1.00
RM	106	1.23	.420	1	2	1.00	1.00	1.00
RM	109	1.26	.439	1	2	1.00	1.00	2.00
RM	109	1.20	.403	1	2	1.00	1.00	1.00
RM	109	1.20	.403	1	2	1.00	1.00	1.00
RM	109	1.29	.458	1	2	1.00	1.00	2.00

Physical Security (PS)

	N	Mean	Std. Deviation	Minimum	Maximum	Percentiles		
						25th	50th (Median)	75th
PS	109	1.13	.336	1	2	1.00	1.00	1.00
PS	111	1.08	.274	1	2	1.00	1.00	1.00
PS	111	1.23	.425	1	2	1.00	1.00	1.00
PS	110	1.35	.478	1	2	1.00	1.00	2.00
PS	107	1.26	.442	1	2	1.00	1.00	2.00
PS	107	1.06	.231	1	2	1.00	1.00	1.00
PS	110	1.14	.345	1	2	1.00	1.00	1.00
PS	105	1.09	.281	1	2	1.00	1.00	1.00
PS	109	1.33	.472	1	2	1.00	1.00	2.00
PS	108	1.51	.502	1	2	1.00	2.00	2.00
PS	109	1.10	.303	1	2	1.00	1.00	1.00
PS	110	1.25	.438	1	2	1.00	1.00	2.00
PS	107	1.19	.392	1	2	1.00	1.00	1.00
PS	105	1.18	.387	1	2	1.00	1.00	1.00
PS	106	1.25	.438	1	2	1.00	1.00	2.00
PS	106	1.30	.461	1	2	1.00	1.00	2.00
PS	110	1.05	.228	1	2	1.00	1.00	1.00

System Security (SS)

	N	Mean	Std. Deviation	Minimum	Maximum	Percentiles		
						25th	50th (Median)	75th
SS	110	1.16	.372	1	2	1.00	1.00	1.00
SS	110	1.09	.289	1	2	1.00	1.00	1.00
SS	109	1.08	.277	1	2	1.00	1.00	1.00
SS	107	1.17	.376	1	2	1.00	1.00	1.00
SS	108	1.19	.398	1	2	1.00	1.00	1.00
SS	108	1.20	.405	1	2	1.00	1.00	1.00
SS	105	1.19	.395	1	2	1.00	1.00	1.00
SS	109	1.16	.364	1	2	1.00	1.00	1.00
SS	109	1.12	.326	1	2	1.00	1.00	1.00
SS	106	1.16	.369	1	2	1.00	1.00	1.00
SS	106	1.21	.407	1	2	1.00	1.00	1.00
SS	105	1.39	.490	1	2	1.00	1.00	2.00
SS	109	1.17	.373	1	2	1.00	1.00	1.00
SS	105	1.10	.308	1	2	1.00	1.00	1.00
SS	109	1.14	.346	1	2	1.00	1.00	1.00
SS	109	1.14	.346	1	2	1.00	1.00	1.00
SS	109	1.39	.489	1	2	1.00	1.00	2.00
SS	107	1.11	.317	1	2	1.00	1.00	1.00

Network Security (NS)

	N	Mean	Std. Deviation	Minimum	Maximum	Percentiles		
						25th	50th (Median)	75th
NS	107	1.23	.425	1	2	1.00	1.00	1.00
NS	108	1.06	.230	1	2	1.00	1.00	1.00
NS	108	1.14	.347	1	2	1.00	1.00	1.00
NS	106	1.20	.400	1	2	1.00	1.00	1.00
NS	107	1.11	.317	1	2	1.00	1.00	1.00
NS	107	1.16	.367	1	2	1.00	1.00	1.00
NS	107	1.15	.358	1	2	1.00	1.00	1.00

Wireless (WI)

	N	Mean	Std. Deviation	Minimum	Maximum	Percentiles		
						25th	50th (Median)	75th
WI	107	1.08	.279	1	2	1.00	1.00	1.00
WI	107	1.13	.339	1	2	1.00	1.00	1.00
WI	107	1.10	.305	1	2	1.00	1.00	1.00
WI	106	1.16	.369	1	2	1.00	1.00	1.00
WI	106	1.24	.427	1	2	1.00	1.00	1.00
WI	104	1.30	.460	1	2	1.00	1.00	2.00
WI	104	1.08	.268	1	2	1.00	1.00	1.00
WI	103	1.18	.390	1	2	1.00	1.00	1.00
WI	105	1.11	.320	1	2	1.00	1.00	1.00
WI	105	1.16	.370	1	2	1.00	1.00	1.00
WI	101	1.15	.357	1	2	1.00	1.00	1.00
WI	104	1.30	.460	1	2	1.00	1.00	2.00
WI	105	1.20	.402	1	2	1.00	1.00	1.00
WI	103	1.08	.269	1	2	1.00	1.00	1.00
WI	103	1.12	.322	1	2	1.00	1.00	1.00

Data Integrity (DI)

	N	Mean	Std. Deviation	Minimum	Maximum	Percentiles		
						25th	50th (Median)	75th
DI	105	1.13	.342	1	2	1.00	1.00	1.00
DI	106	1.08	.265	1	2	1.00	1.00	1.00
DI	103	1.12	.322	1	2	1.00	1.00	1.00
DI	105	1.16	.370	1	2	1.00	1.00	1.00
DI	102	1.10	.299	1	2	1.00	1.00	1.00
DI	106	1.10	.306	1	2	1.00	1.00	1.00
DI	105	1.14	.352	1	2	1.00	1.00	1.00
DI	105	1.30	.463	1	2	1.00	1.00	2.00