2019

Factors Affecting Perceptions of Cybersecurity Readiness Among Workgroup IT Managers

Thomas A. Chapman
University of Mississippi

Factors Affecting Perceptions of Cybersecurity Readiness Among Workgroup IT Managers

A Dissertation
Presented in Partial Fulfillment of Requirements
For the degree of
Doctor of Philosophy in Business Administration
Management Information Systems
The University of Mississippi

By:

Thomas A. Chapman
December 2018

ABSTRACT

The last decade has seen a dramatic increase in the number, frequency, and scope of cyberattacks, both in the United States and abroad. This upward trend necessitates that a significant aspect of any organization's information systems strategy involves having a strong cybersecurity profile. Inherent in such a posture is the need to have IT managers who are experts in their field and who are willing and able to employ best practices and educate their users. Furthermore, IT managers need to have awareness of the technology landscape in and around their organizations. After many years of cybersecurity research, large corporations have come to implicitly understand these factors and, as such, have invested heavily in both technology and specialized personnel with the express aim of increasing their cybersecurity capabilities. However, large institutions are comprised of smaller organizational units, which are not always adequately considered when examining the cybersecurity profile of the organization. This oversight is particularly true of colleges and universities where IT managers who are not affiliated with the institution's central IT department employ their own information security strategies. Such strategies may or may not represent a threat to the institution's overall level of cybersecurity readiness. Therefore, this research examines the responses of workgroup IT managers who are employed at the school or department level at institutions of higher learning within the United States to determine their perceptions of their cybersecurity readiness. The conceptual model that is developed in this study is referred to as the Practice and Awareness Cybersecurity Readiness Model (PACRM). It examines the relationships between an IT

manager's perceived readiness to detect, prevent, and recover from a cyberattack, and four base factors. Among the factors studied are the manager's previous level of experience in cybersecurity, the extent of the manager's use of best practices, the manager's awareness of the network infrastructure in and around the organizational unit, and the degree to which the manager's supported user community is educated on topics related to information security. First, a survey instrument is proposed and validated. Then, a Confirmatory Factor Analysis (CFA) is conducted to examine the relationships between the observed variables and the underlying theoretical constructs. Finally, the model is tested using path analysis. The validated instrument will have obvious implications for both cybersecurity researchers and managers. Not only will it be available to other researchers, it will also provide a metric by which practitioners can gauge their perceptions of their cybersecurity readiness. In addition, if the underlying model is found to have been correctly specified, it will provide a theoretical foundation on which to base future research that is not dependent on threats and deterrents but rather on raising the self-efficacy of the human resource.

DEDICATION

This dissertation is lovingly dedicated to
Desi and Lily both, who were generous with their
patience, gracious with their love and hugs,
and unsparing in their support and
encouragement. Truly it must be said that
this dissertation was a family endeavor.

LIST OF ABREVIATIONS AND SYMBOLS

ARPA	Department of Defense Advanced Research and Projects Agency
AVE	Average Variance Extracted
CEH	Certified Ethical Hacker
CFA	Confirmatory Factor Analysis
CFI	Comparative Fit Index
CIO	Chief Information Officer
CNA	Computer Network Attack
CND	Computer Network Defense
CNE	Computer Network Exploitation
CSE	Computer Self-Efficacy
CR	Composite Reliability
EFA	Exploratory Factor Analysis
EUC	End-User Computing
GDT	General Deterrence Theory
ISP	Information Security Policy
KMO MSA	Kaiser-Meyer-Olkin measure of sampling adequacy
MIS	Management Information Systems
MSV	Maximum Shared Variance
MTMM	Multi-Trait Multi-Method

N.S.A.	National Security Agency
NFI	Normed Fit Index
PACRM	Practice and Awareness Cybersecurity Readiness Model
PCA	Principle Component Analysis
PHCS	Perceived Health Competence Scale
RMSEA	Root Mean Square Error of Approximation
SaaS	Software-as-a-Service
SAC	Security Action Cycle
SEM	Structural Equation Modeling / Security Event Management
SET	Self-Efficacy Theory
SIM	Security Information Management
SIEM	Security Information & Event Management
SRMR	Standardized Root Mean Square Residual
SRS	Security Related Stress
TPB	Theory of Planned Behavior
TRA	Theory of Reasoned Action

ACKNOWLEDGMENTS

As my advisor remarked upon hearing one of the conclusions of this research, “it takes a village to fend off a cyberattack.” Truly, the same must be said of any dissertation project. The current document is no exception to that general rule.

I would, therefore, like to begin by acknowledging the innumerable contributions of my dissertation chair and faculty advisor, Dr. Brian Reithel, to this research. I first met Dr. Reithel when I burst into his office in the summer of 2014 making the case that my undergraduate degree in CIS had thoroughly prepared me for the doctoral program in MIS, despite my recent and prolonged sojourn into the realm of history. Truth be told, I was a little taken aback that my pitch seemed to work. He encouraged me to apply to the program. In retrospect, I see that Dr. Reithel was willing to take a chance on me. At times, it must have seemed like long odds indeed. Dr. Reithel took it upon himself to teach me, not only the ins and outs of the conceptual model development process, but also to impress upon me the responsibilities of accepting a role in academia. Through his example, he helped to show me how to be a good faculty member and how to contribute to society through my work, both as a teacher and as a scholar.

Dr. Tony Ammeter and Dr. Bart Garner were two of my earliest mentors in the program. I worked for Dr. Ammeter as his teaching assistant during my first semester under assistantship. He helped me to see the relevance of what I was doing in terms of how it impacted my student’s lives. I am a better teacher now because of my time spent as his T.A. Later, he showed me how to incorporate theory into my work in a meaningful and impactful way. Meanwhile, Dr. Garner

was my M.B.A. instructor during my second semester in the program. He graciously shared of his time and expertise to show me how an M.B.A. class should be structured. Having elected to get my master's degree in, of all things, American history, I had no concept of what an M.B.A. class should look like, much less how to get one to run smoothly. Thanks to Dr. Garner, I have a model and resources from which to draw, and I know that knowledge will be invaluable to me as I progress through my faculty career. As a cybersecurity specialist, Dr. Garner's expertise in refining key aspects of the model was indispensable.

Lastly, Dr. John Bentley graciously served on my committee as the external member. This was no small feat since I am reasonably confident that Dr. Bentley was simultaneously serving on every other doctoral student's committee at the University of Mississippi. However, as John is wont to recall, he's known me since the beginning, since before I was a Ph.D. student in the history program much less the MIS program. We were colleagues when I first started working for the university and I knew him simply as a department professor, already in the final stages of completing his second Ph.D. Now that he is the department chair and his office has gotten a little bigger, I marvel at the speed with which he can find any one study among the teetering stacks of paper that are his filing system. He is the consummate professor as well as a friend. For that, as well as for the uncounted number of times that he has provided a listening ear or complex statistical advice, I owe him more than I can ever say.

Although she did not serve as a member of my committee, Dr. Sumali Conlon was invaluable to my success as an MIS doctoral student. I will always remember, with great

fondness, her seminars on databases and artificial intelligence where she honed our presentation skills amid banter of good food and the joys of traveling.

The contributions of Dr. Robert Van Ness cannot, and should not, be left unacknowledged. The man had to field innumerable emails from me requesting cubicle changes to the point where I am sure he merely threw a dart at a board rather than throw it at me, as he was no doubt inclined to do. His patience is his true legacy. Dr. Milam Aiken, the MIS department chair, was always generous in finding the funds for me to travel to one research conference or another and was likewise always available when I needed his help. I could not have been a scholar without him. Finally, the contributions of the School of Business administrative staff; Teresa Rowsey, Becky Kesler, Susie Potts, Amy Johnson, and Sam Hammoud, as well as many others, cannot be overstated. They had to endure much, but they prevailed! Thank you, all.

Sincerely,

Thomas A. Chapman

CONTENTS

LIST OF TABLES

LIST OF FIGURES

1 INTRODUCTION

1.1 Cybersecurity Today

We are now treated to almost daily accounts of some new cyber or ransom ware attack. Each intrusion that we read about in the morning paper, such as the recent cyberattack against Equifax, endangers the personal information of hundreds of millions of individuals (Bernard, et al., 2017). In some cases, the ability of life-saving institutions to function at full capacity is threatened, thereby endangering human lives (Barts Health NHS Trust, 2017). Due to the enormity and rapid deployment of today's cyber and ransom ware attacks, it can be difficult to come to terms with what, if anything, can be done to stop the seemingly endless tide of such events.

In addition to the Equifax data breach, a major recent event was the global ransomware known as the WannaCry virus, which swept across the globe in a matter of hours paralyzing computers in approximately 150 countries (Sanger, Chan, & Scott, 2017). Other recent cyberattacks, although less publicized than the WannaCry attack, have run the gamut from the mundane to the bizarre (Perlroth & Haag, 2017; Rosenberg & Salam, 2017). These incidents all clearly demonstrate that cyber and ransom ware attacks are increasing worldwide in frequency, scope, and severity. This trend is driven by the relative ease with which hackers can now launch a world-wide cyber attack; a trend that has been made possible by the confluence of new and widely-available tools, which have combined to make cyber and ransom ware attacks both easy and profitable. As Nicole Perlroth notes in her New York Times article entitled, "With New

Digital Tools, Even Nonexperts Can Wage Cyberattacks," the advent of digital currencies like BitCoin, together with the proliferation and adoption of new and powerful encryption software, have made it increasingly easy for would-be thieves to wage cyber and ransom ware warfare. Perlroth notes, for example, that the WannaCry attack, which started in Europe on the afternoon of May 12, 2017, was an escalation of recent previous episodes, which exploited the same Microsoft Windows vulnerability that was first discovered by the National Security Agency (N.S.A.) of the United States. The exploit became available to hackers in April, 2017 when a group called the "Shadow Brokers" targeted the N.S.A. and made away with several of the agency's own hacking tools. One of those tools, code-named EternalBlue, formed the basis for the WannaCry ransom ware. Microsoft Windows is the operating system of choice for approximately 80% of the world's desktop computers. Even though Microsoft had been warned by the N.S.A. prior to May, 2017 that the exploit had been exposed and was available to hackers, and Microsoft had in turn released a security patch to close the exploit, enough computers were left exposed that the WannaCry ransom ware was able to encrypt the computers of more than 70,000 organizations before it was stopped (Perlroth, 2017[b]). Perlroth further notes that several of the Bitcoin accounts associated with the ransom ware received the equivalent of $33,000 American dollars by May 13, 2017 for an attack, which had begun the previous afternoon. By the following Monday, the Bitcoin payments totaled just under $60,000 (Lohr & Alderman, 2017).

Fortunately, cybersecurity specialists are as qualified and motivated as hackers are. Take, for example, the story of the young cybersecurity expert who worked from his bedroom flat in England to stem the tide of the WannaCry attack. Marcus Hutchins, a 22-year old English tech worker who works for the Los Angeles-based security firm Kryptos Logic, was analyzing a

sample of the malicious code that made up the WannaCry virus when he noticed that the code referenced an unregistered web domain. He promptly registered the domain, which helped to slow the spread of the attack. The CEO of Kryptos Logic, Salim Neino, credits Hutchins with slowing the virus on Friday afternoon European time before it could infect computers in the United States. Neino was effusive in his praise of Hutchins' work, stating that, "Marcus, with the program he runs at Krypto Logic, not only saved the United States but also prevented further damage to the rest of the world" (The Associated Press, 2017). Later, a kill switch was created by Matthieu Suiche, another cyber security researcher, to stop the virus (Perlroth, Scott, & Frenkel, 2017). Hutchins and Suiche are part of a global network of security specialists who watch for cyber threats to emerge and work to thwart them. Those specialists are part of a global industry that, it is estimated, will spend over $120 billion in 2017, up from just $3.5 billion in 2004. That growth is projected to continue at twelve to fifteen percent annually for the next five years (The Associated Press, 2017). Such resources will be increasingly important, since the WannaCry ransom ware attack by no means represents the zenith of the worldwide cyber and ransom ware threat.

Indeed, many cybersecurity specialists believe that we are already seeing the next evolution of attacks based on the tools that were stolen from the N.S.A. On April 29, 2017, a cyberattack hit the IDT corporation. That company's global chief information officer is a cyber security specialist by the name of Golan Ben-Oni. That attack presented itself as a ransom ware attack. However, further analysis indicated that the ransom ware was simply a mask to cover the deployment of a second tool, which had also been stolen from the N.S.A. earlier in the month. The tool, which is code-named DoublePulsar, allows hackers to insert malicious code into the kernel of a computer's operating system, effectively bypassing many standard cyber security

measures. In the intervening months since the attack, Mr. Ben-Oni stated that he has spoken with over a hundred security experts in all facets of the industry, including chief executives of nearly every major security company as well as the heads of intelligence at Google, Microsoft, and Amazon. Of those firms, only Amazon had found traces of a residual probing effort by the same computer that hit IDT. DoublePulsar represents a new and pervasive level of cyber threat. Sean Dillon, an analyst at RiskSense, a New Mexico-based cyber security firm, tested all major antivirus products against the DoublePulsar hack and found that 99% of the them failed to detect it (Perlroth, 2017[a]).

A second large-scale cyberattack hit the Ukraine on June 27, 2017 and immediately spread internationally. It used the same Microsoft Windows exploit, EternalBlue, that the WannaCry ransom ware attack used. The more recent attack, however, was more encompassing in that it worked by encrypting the entire hard drive of the computer, whereas the WannaCry virus targeted only individual files and directories. The attack crippled ATM machines in Kiev and radiation monitoring stations at Chernobyl where workers were forced to monitor radiation levels manually. In the United States, hospitals in two cities in Pennsylvania were forced to temporarily shut down operations after the attack affected computers at Heritage Valley Health Systems, a Pennsylvania health care provider. The attack spread through both the Microsoft Windows exploit and through stealing users' credentials in much the same way as the attack on IDT did. This means that even computers that had the latest Microsoft patch might have been vulnerable to infection. In this way, the attack shared many similarities with a virus that emerged last year called Petya. Petya, which translates to "Little Peter" in Russian, was available for sale on the "Dark Web" where it was sold as "ransom ware as a service," a play on Silicon Valley's business model of software-as-a-service (SaaS). This made it difficult to trace

the individuals responsible for the attack. It is relatively easy, for example, for purchasers of the service to encrypt victims' computers and demand a ransom, which the creators of the original Petya virus then receive a portion of (Perlroth, Scott, & Frenkel, 2017).

1.2 Cybersecurity: History and Definitions

The first known usage of the term cybersecurity was in 1989. It is simply defined as, "any measures taken to protect a computer or computer system against unauthorized access or attack" (Merriam-Webster, 2017). Information security, or computer security, however, describes a concept that emerged with the development of the first mainframe computers in the 1960s. In June 1967, researchers at the Department of Defense Advanced Research and Projects Agency (ARPA) began meeting regularly to discuss security of classified information. The group was made official in October 1967 and was immediately tasked with formulating recommendations (Whitman & Mattord, 2016). Those recommendations formed the basis for the Rand Report R-609, which was later declassified in 1979 under the title Rand Report R-609-1. Rand Report R-609-1 became the first widely accepted document to identify management and policy issues surrounding information and computer security (Ware, 1979).

Research into the subject of computer security continued throughout the 1970s. However, with the migration of computers out of the controlled and physically isolated mainframe environments and into the organization, research into computer security took on a new urgency. As such, there was a movement during the latter half of the 1980s to redefine what information security meant (Brancheau & Wetherbe, 1987). A slightly more comprehensive definition, therefore, may be found in a 1988 treatise on building a secure computer system. The author states that information security is, "the protection of computer systems against the theft or damage to their hardware, software, or information, as well as from disruption or misdirection of

the services they provide" (Gasser, 1988). Information security, within this context, involves controlling access to the physical hardware of the computer as well as protecting against threats that may originate from outside the physical infrastructure; through the manipulation of network access, for instance.

1.3 Problem Statement

According to a recent survey of Chief Information Officers (CIOs), organizational information security is at the forefront of their management concerns (Grant Thornton, 2016). Despite this fact, however, and despite a spate of security management research that focuses on commercial organizations, there seems to be a relative absence of applicable research as it pertains to complex, multi-tiered organizations such as colleges and universities. Studies that specifically examine the link between cybersecurity and higher education seem to be limited to just a few, which took place primarily in the decade between 2000 and 2010. (Elliott et al., 1991; Rezgui & Marks, 2008; Tout et al., 2009; Oblinger & Hawkins, 2006). This lack of recent inquiry persists despite evidence that institutions of higher learning are experiencing cyberattacks with increased frequency (Rezgui & Marks, 2008).

Research into the cybersecurity readiness of colleges and universities is complicated by the distributed nature of IT administration at such institutions. While much of the responsibility for the management of an institution falls under the purview of the central IT department, numerous responsibilities still reside within individual schools and departments. The men and women who shoulder these responsibilities often work outside of the central department. As such, it follows that they neither share in the department's resources nor in its organizational hierarchy. The actions of such school and department level managers may represent an uncontrolled variable in the organization's cybersecurity profile, which in turn presents a potential avenue of exploitation

for individuals who are intent on gaining unauthorized access to that institution's information resources. For these and other reasons, institutions of higher learning, especially at the school or department level, are an important, but neglected, area of inquiry in terms of information security research. Since decentralized IT administration is a trait that is common to many complex, multi-tiered organizations, a comprehensive evaluation of the factors most associated with cybersecurity readiness at this level is needed. It is the view of this project that such an evaluation should take place within the context of colleges and universities to address the relative paucity of research pertaining to that domain. This study therefore attempts to fill that void by examining the behavior and perceptions of workgroup IT managers who work at the school and department level of colleges and universities in the United States.

1.4 Research Questions

We begin by asking the following research question:

RQ1: What factors are associated with the perceived readiness of workgroup IT managers to detect, prevent, and if necessary, recover from a cyberattack?

By answering *RQ1*, this project hopes to more thoroughly address the topic of cybersecurity readiness in complex, multi-tiered organizations. From a comprehensive review of the relevant information security research, it was hypothesized that four distinct groups of factors help to inform an IT manager's perceived cybersecurity readiness. These four factors are: the manager's previous level of experience with cybersecurity, the extent of his or her use of known best practices, his or her perceived awareness of several factors related to the network and computer infrastructure, and the degree to which the user community that he or she supports is educated about issues related to information security. Therefore, a subset of research questions related to *RQ1* is:

RQ1a: How is an IT manager's previous level of cybersecurity experience related to his or her perceived readiness to detect, prevent, and recover from a cyberattack?

RQ1b: How is the extent of an IT manager's use of cybersecurity best practices related to his or her perceived readiness to detect, prevent, and recover from a cyberattack?

RQ1c: How is an IT manager's awareness of the network environment in and around the organizational unit related to his or her perceived readiness to detect, prevent, and recover from a cyberattack?

RQ1d: How is the degree to which the user community is educated about issues pertaining to information security related to the IT manager's perceived readiness to detect, prevent, and recover from a cyberattack?

Finally, a manager's attitude toward risk should be also be considered when evaluating the extent of his or her use of best practices. Therefore,

RQ2: Does attitude towards risk affect the relationship between an IT manager's previous level of experience and the extent of his or her use of cybersecurity best practices?

To answer these research questions, the following theoretical model was developed. It will be described and validated throughout the remainder of this dissertation.

1.5 PACRM Theoretical Model

This project develops and evaluates a model, which links the four factors listed above with the IT manager's perceived readiness to detect, prevent, and recover from a cyberattack. The model is illustrated below in Figure 1.

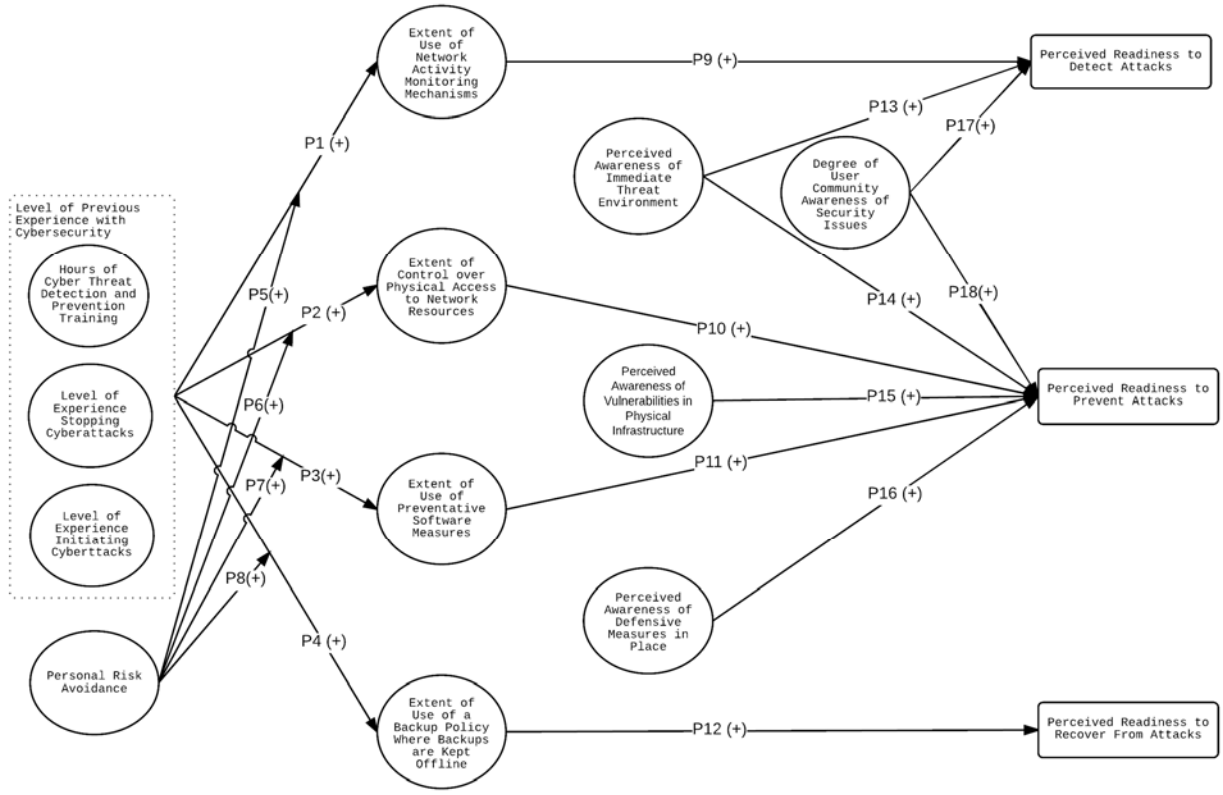

Figure 1: PACRM Conceptual Model Diagram

Level of Previous Experience with Cybersecurity is a summative measure, which is composed of three distinct variables. The first variable is the amount of time that the manager has spent engaged in cyberattack detection and prevention training. This variable is combined with the manager's self-reported levels of experience with stopping and initiating cyberattacks. This factor is thought to be related to the *Extent of Use* factors, which capture the manager's use of network activity monitoring mechanisms, the extent of control over physical access to computer and network resources, the use of software preventative measures, and the use of a backup policy where backups are kept offline. Next, the *Perceived Awareness* factors capture the manager's knowledge and awareness of the immediate threat environment, the perceived vulnerabilities in the physical network infrastructure, and the defensive measures currently in place to protect against intrusion. Third, the *Degree of User Community Awareness of Security*

Issues factor represents the IT manager's perception of the degree to which the user community that he or she supports is educated about issues related to information security. Finally, the manager's attitude towards risk, as denoted by a risk avoidance measure, moderates the relationship between his or her previous level of experience with cybersecurity and the extent of his or her use of best practices.

1.6 Review of Methodology

To test the PACRM theoretical model in Figure 1, it is first necessary to develop a survey instrument that can be administered to the appropriate managers. Since the instrument is new, it must first undergo a process of instrument validation. The final survey instrument is included as Appendix C of this document.

The validation of the PACRM measurement instrument will be conducted in three stages. Stages 1 and 2 comprise the pilot test phase while stage 3 represents the roll-out phase. Stage 1 will consist of qualitative interviews with several IT managers at a large, public university in the southeastern United States. Researcher notes of each of the interviews will be collected and the answers correlated to establish relevant content validity. The interviewees will then be administered the PACRM survey on paper and encouraged to "think aloud" as they record their answers. This is an effort to begin establishing the construct validity of the proposed instrument by noting which questions pose a difficulty for the participants.

Stage 2 will consist of the revised survey being administered as a web-based, Qualtrics study to IT managers working at colleges and universities throughout the southeastern United States. The resulting data will be analyzed, and Cronbach's alpha statistics will be generated to test the reliability of the proposed instrument.

Finally, stage 3 will comprise the roll-out phase of the instrument to workgroup IT managers working at institutions of higher learning throughout the United States. Once enough responses are generated, a CFA will be done to see how closely the survey aligns with the theoretical assumptions of the underlying PACRM model. Lastly, the proposed relationships in the model will be tested using a path analysis framework.

1.7 Chapter Overview

Chapter one provided a brief overview of the state of cybersecurity today. It identified a problem in the current cybersecurity literature. Namely, even though past and contemporary studies have affirmed the primacy of cybersecurity among the concerns of top organizational managers, the extant information security literature has not dealt extensively with organizational-unit level analyses, such as are needed for institutions of higher learning. Therefore, this dissertation argues that a new model is needed that can be applied equally as well to any institution that exhibits a decentralized IT organizational structure. Chapter 1, therefore, introduced and briefly described the Practice and Awareness Cybersecurity Readiness Model (PACRM), which will be discussed and validated through the remainder of this project.

Chapter two goes through a review of the scholastic literature pertaining to organizational cybersecurity. Starting in the late 1980s and early 1990s, researchers began to look at the issue of organizational computer security in earnest. Inquiry into the domain of computer security began with several surveys noting areas of concern among organizational managers. These surveys initially ranked computer security high among managers' concerns. However, as the end-user computing revolution moved computing resources out of the mainframe environment and into the micro-computer and networking environments, managers struggled with how to conceptualize information security, and the issue moved down their list of concerns. Beginning

in the early 1990s, several researchers took up the mantle of researching organizational security. Over the course of this research, several informative conceptual models were developed and tested. Goodhue and Straub (1991) developed a theory and empirical-based model, which looked at managers' perceptions as a function of industry risk, the extent of organizational effort to control those risks, and individual factors such as awareness of previous system violations, and security background. That model has many elements in common with the PACRM model being proposed in the present research. Later research began to look at information security as a function of manager behavior. Specifically, research that was based on the Theory of Planned Behavior (TPB) played a significant role in identifying factors that could shape IT managers' information security intentions. Chapter two concludes by describing the theoretical and empirical foundations of the variables in the PACRM model, which has determinants, like models before it, in General Deterrence Theory (GDT). However, GDT-based research, which can end up relying heavily on technologically-driven solutions to ensure both the certainty and severity of sanctions, has been shown to be inadequate in some cases (Cavusoglu, Son, & Benbasat, 2009; Dhillon & Backhouse, 2001). Therefore, Self-Efficacy Theory (SET) is used, in conjunction with general deterrence theory, to inform the remainder of the components of the PACRM model.

Chapter three describes the proposed relationships between the independent factors and the dependent factors of the PACRM model. Those relationships are then articulated in the form of propositions.

Chapter four discusses the proposed survey instrument in detail. The stages of instrument validation are discussed, and a survey methodology is articulated. As described above, in the pilot testing phase, the survey will first be administered to several IT managers who work at the

school or department level of several colleges and universities located in the United States. The initial stage consists of qualitative interviews with several IT administrators who work at a large university in the southeastern United States. These administrators ranged in years of professional IT work experience from 5 to 39 years. The results of those interviews resulted in the inclusion of a new factor into the original model, and a new block of questions on the survey instrument. In stage two of the pilot study, the survey was administered as a web-based, Qualtrics survey to several college and university IT administrators. Reliability statistics were generated and analyzed. Stage three consisted of a national survey of IT administrators drawn from the collegiate and university workgroup IT manager population. Confirmatory factor analysis was used to determine the extent to which the survey instrument matched expectations generated from the underlying model. Once the CFA analysis is complete, the data from stage 3 was used to conduct a path analysis to determine whether the conceptual model adequately describes managers' perceived readiness to detect, prevent, and recover from a cyberattack.

2 LITERATURE REVIEW

In a recent survey of 210 security professionals by a leading security platform provider, it was found that, on average, ten percent of security personnel admitted to having paid a ransom or having hid a security breach from their associates or supervisors to protect their jobs (Bromium, 2017). This research is in line with previous studies, which found that *insiders*, a term that has been used to describe employees who are authorized to use organizational systems, facilities, or computer resources, may pose a risk to those organizations' computer security (Neumann, 1999; Warkentin & Willison, 2009). In addition, previous studies have found that deliberate acts, such as those described above, can significantly impact information security (Lee & Lee, 2002; Lee et al., 2004).

2.1 The Rising Importance of Information Security

Research studies that documented threats to computer systems began in earnest as early as the mid-1970s and have continued through the present day (Parker, 1976, 1981, 1983; Loch, Carr, & Warkentin, 1992; Whitman, 2004). Early high profile studies and reports primarily documented threats against the U.S. government (Colton et al., 1982; Kusserow, 1983). However, it did not take long for researchers and executives to recognize the significance of information security to businesses. In the mid-1980s, researchers working out of the University of Minnesota began exploring the issues of greatest concern to information systems executives and corporate managers (Dickson, et al., 1984; Brancheau & Wetherbe, 1987). They found that

strategic planning and using computers for competitive advantage were at the forefront of executives' minds. Organizational learning and IS's role and contribution to the organization were also among their concerns, foreshadowing the increasing importance of End-User Computing (EUC) to organizations. The rising importance of information security, however, can be seen in such studies by the relative value that executives placed on data as a corporate resource (Brancheau & Wetherbe, 1987).

The Brancheau and Wetherbe (1987) study is particularly interesting both in terms of its survey method and its results. Previous studies (Ball & Harris, 1982; Hartog & Herbert, 1986) had found that information security ranked much higher among the member populations they studied. The relative discrepancy in rankings between the studies is likely an artifact of the survey methods the researchers used and the populations they studied. For instance, in their survey, Hartog & Herbert employed a single-round cross-sectional approach while Brancheau and Wetherbe used a three-round Delphi study. It is important to note that the issue of computer security would come to much rank higher in subsequent studies of the kind (Brancheau, Janz & Wetherbe, 1996; Ransbotham & Mitra, 2009). Brancheau & Weatherbe acknowledge this possibility in 1987 when they remark in their closing statements that, "While it is useful to make a periodic assessment of what IS professionals feel are the profession's most critical issues, it is often the less obvious problems that become major concerns."

2.2 General Deterrence Theory-based Research

The veracity of that statement was already beginning to assert itself within just a few short years. Detmar Straub, a researcher who was also working out of the University of Minnesota at the time, began to argue for the importance of information security as early as 1990. Based on research he had done previously (Hoffer & Straub, 1989; Straub & Hoffer,

1987), it was apparent to Straub that organizations were not giving the issue of information security the requisite attention he felt it deserved, despite the stated importance of data as a corporate resource. In response, Straub undertook research that looked at information security from the perspective of General Deterrence Theory (GDT) (Straub D. W., 1990). His research indicated that investment in IS research could significantly reduce incidents of computer abuse by advocating for the use of countermeasures, which included administrative policies aimed at deterrence. Straub's data also showed that data security activities, which he defined as electronic security measures, were integral to decreasing the number of incidences of computer abuse within the organizations that he surveyed.

The applicability of security countermeasures for reducing incidents of computer abuse had been studied in the Information Systems literature prior to Straub's research (Madnick, 1978). However, Straub's aim was to not only to determine if IS deterrence was effective in reducing incidences of computer abuse, but also to determine if rival explanations, such as the use of security software, could explain lower incident rates of computer abuse (Straub D. W., 1990). In order to do so, he defined computer abuse in the traditional vein (Kling, 1980) as abuse perpetuated by individuals against organizations. Straub articulated that abuse could occur in this context as *hardware* abuse, *software* abuse, *data* abuse, and *computer service* abuse (1990). These four aspects of information security would later form the basis for many cybersecurity related protocols and frameworks such as COBIT 5, ISA 62443-2-1:2009, ISO/IEC 27001:2013, and NIST SP 800-53 Rev.4 (NIST, 2014). In addition, Straub's research represents one of the first empirical studies to validate the effectiveness of security software in preventing incidents of computer abuse.

Later that same year, Straub and another researcher co-authored a study, which addressed the way in which IS security managers uncovered incidences of computer abuse and disciplined computer abusers (Straub & Nance, 1990). The authors' goal for the project was to develop a way of assessing the risks that organizations face as well as the measures being taken by organizations to detect computer abuse and discipline abusers. A by-product of this research was to identify information security managers' contemporary responses to computer abuse and to determine factors that could help those managers reduce incidents of computer crime.

Previous research (Straub, 1986) had found that two classes of counter measures – deterrents and preventatives – were shown to be successful in reducing incidents of computer abuse. Deterrents, as defined by the author, passively restrict the use of computer resources and include actions such as computer security training sessions and policy statements. Preventatives, on the other hand, are those actions that actively restrict the use of computer resources. These may include things like physical barriers to locations where sensitive data or computer resources are kept and software solutions such as firewalls and passwords. Detection is another important component of deterrence. Parker (1981) defined detection as the intentional investigation of system activity in order to identify irregularities. The principle would later find application in Dorothy E. Denning's work on Intrusion Detection Systems (1987). Straub and Nance found that incidents of computer abuse were discovered in three general ways; through accidental discovery, normal system controls, and purposeful investigation. The incidents that were identified from their survey were overwhelmingly discovered by accident, or through normal system controls (1990). Sadly, detection of extant threats through purposeful investigation remains the most challenging aspect of cybersecurity to this day.

Goodhue & Straub (1991) looked at ways in which managers could develop a sense for the proper balance between exposing their department to unnecessary risk and the cost associated with preventative measures. The authors argued that managerial concern over organizational security is a function of the risk that is inherent in the industry, the extent to which the organization has controlled for these risks, and the factors that are associated with the individual managers, such as their awareness of previous systems violations and their level of experience in performing systems control work. Goodhue and Straub's model is shown in Figure 2 below.

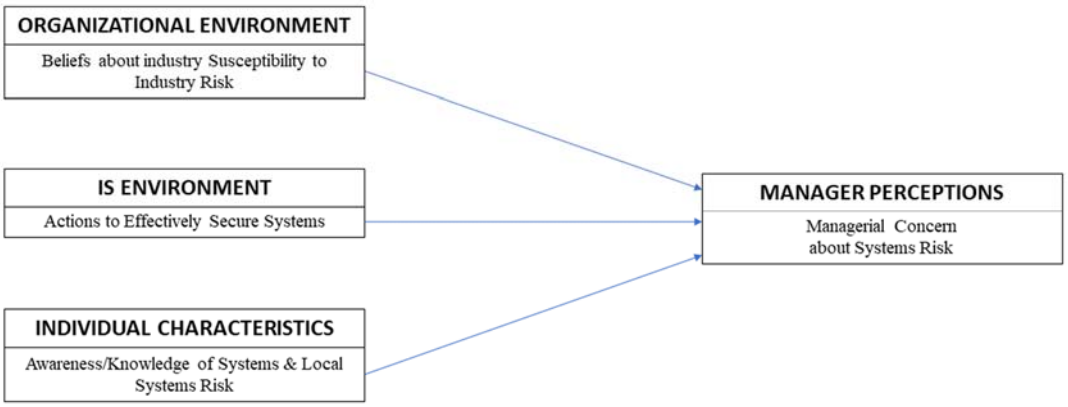

Figure 2: Managerial Perceptions of Security Risk (Goodhue & Straub, 1991)

Several elements from Goodhue's and Straub's model have correlations in the PACRM model being proposed herein. The second and third components, "IS Environment" and "Individual Characteristics," in particular, are both related to elements of the proposed model that is described below in Chapter 3. As stated by Goodhue and Straub, the "IS Environment" construct reflects managers' current understanding of the type of technical and managerial controls that can be used to secure information systems. The "Individual Characteristics" component, meanwhile, describes how well informed managers are about the number and types of local security incidents and the susceptibility of their systems to damage (Goodhue & Straub, 1991). As their research showed, both factors are informative in determining managers' concern

about systems risk. In fact, independent corroboration of Goodhue & Straub's proposed relationships was reported shortly after the paper was originally published (Dixon, Marston, & Collier, 1992). However, both constructs were designed to be very high level in how they assessed individual managers' awareness/knowledge. Neither factor addressed specific areas of concern to IT managers. In addition, Goodhue & Straub's research was designed to measure manager perceptions at the executive level. As such, their model has the implicit assumption that managerial concerns about IS security are only relevant at the institutional level. Such research is unquestionably valid. However, as stated in the introduction, the present research addresses the perceptions of IT managers at the decentralized level of administration. This is important because measuring manager perceptions at this lower level of IT administration has important ramifications for the cybersecurity profile of the institution as a whole.

In 1998, Straub and Richard Welke collaborated to test their Security Action Cycle (SAC) model using qualitative data that they obtained from two Fortune 500 firms. Previous research had emphasized four distinct categories related to information security. These categories were deterrence, prevention, detection, and recovery (Forcht, 1984; Parker, 1981). Straub and Welke's model looked at a possible method of deterrence feedback, based on a series of sequential actions that managers could take. These actions ranged from deterrence to remediation (Straub & Welke, 1998). While informative, the model is primarily concerned with reinforcing the two central tenets of general deterrence theory, which are the certainty and severity of punitive actions to deter abusive behavior. However, GDT-based solutions, like the ones presented above, while arguably the dominant framework for security research throughout the 1990s, do not represent the sum total of information security research.

In fact, there have been several recent critiques of GDT-based research. In 2011, researchers sought to understand the relationship between the punishment of Information Security Policy (ISP) breaches by insiders and the perceived justice of those punishments (Xue, Liang, & Wu, 2011). They found that the intention to comply with the organization's security policy is strongly related to the perceived justice of punishment, which in turn is negatively affected by actual punishment. Because punishment serves to enforce the two key tenets of general deterrence theory, as articulated in Straub's original article (1990), Xue et al.'s findings represent a significant repudiation of the effectiveness of GDT-based solutions. Additional research has examined the role that computer monitoring plays on attributed trust (Posey, Bennett, & Roberts, 2011). Attributed trust is the insider's perception that the organization trusts them. The authors found that low attributed trust drives incidents of computer abuse. Likewise, it has been found that security related stress (SRS) from security controls may adversely affect moral engagement among employees and, in turn, lead to increased incidents of computer abuse (D'Arcy, Herath, & Shoss, 2014). While GDT-based studies may no longer be at the pinnacle of insider threat research, they do represent an important foundational step for subsequent research that looked at these issues (Mitnick & Simon, 2002; Warkentin & Willison, 2009). However, to go further, information security research had to evolve beyond simple deterrence to begin to address individual intention as well.

2.3 Theory of Planned Behavior-based Research

In 2010, researchers from the University of British Columbia continued the examination of employee behavior regarding information security by also looking at employee compliance with ISPs. Rather than adopting a GDT perspective, however, they did so from the vantage point of the Theory of Planned Behavior (TPB) (Ajzen, 1991). TPB postulates that an individual's

intention to perform various kinds of behaviors can be predicted by his or her attitudes towards the behavior, subjective norms, and perceived behavioral control, which are all original aspects of the Theory of Reasoned Action (TRA) (Ajzen & Fishbein, 1980; Fishbein & Ajzen, 1975). TPB further stipulates that behaviors can be explained through behavioral beliefs, normative beliefs, and self-efficacy, which serve as antecedents to attitudes, subjective norms, and behavioral control (Bulgurcu, Cavusoglu, & Benbasat, 2010).

A good example of information security research that is based on TPB is Bulgurcu et al.'s article, which postulated that employees' intention to comply with their organization's ISP is influenced by three factors: attitude towards compliance, normative beliefs, and self-efficacy (2010). In that article, the authors researched the role that the employee's information security awareness plays in shaping his or her attitude toward compliance. They postulated that it influences his or her beliefs over the outcome as well as his or her attitude toward compliance. In turn, his or her attitude towards compliance informs his or her intention to comply with the organization's ISP. Bulgurcu et al.'s model is informative. However, one area of concern with respect to their model is that "Information Security Awareness" is comprised only of the manager's awareness of the organization's ISP and the manager's general security awareness. As with Goodhue & Straub's model from Figure 2 above, the constructs are not grounded in specific areas of concern to IT managers. While it was not the authors' intention to incorporate specific areas of awareness, other than ISP awareness, into their model, it is nonetheless an area that this dissertation seeks to address.

In 2009, Dinev et al. (2009) also looked at user behavior and attitudes towards protective information technologies from a TPB perspective. They posited that cultural differences moderate the strength of the relationship in the traditional behavioral model within the context of

these technologies. Specifically, they found a moderating effect when they examined data from two divergent cultures, the United States and South Korea. The authors argue that their findings indicate that cultural differences need to be taken into account when designing certain classes of protective technologies such as spyware-detection software.

2.4 Research with other Theoretical Orientations

Boss & Kirsch (2007) looked at ways to motivate employees to follow corporate security guidelines by adopting an organizational lens approach. In their paper, the authors introduce the concept of "mandatoriness," which they define as the degree to which employees perceive that compliance with the organization's information security guideliness is expected, or mandatory. They found that through the specification of policies and evaluation of employee behavior, firms can be effective in convincing their employees that security policies are mandatory, and that compliance, therefore, is compulsory. In turn, the perception of mandatoriness among employees is effective in motivating them to adopt security practices. Although presented as a novel concept, "mandatoriness" has much in common with the theoretical assumptions of GDT-based perspectives. Additional research has argued that employees' moral reasoning and values affects their compliance with their organizations' information security policy (Myyry et al., 2009). The authors' theory is based on two existing theories of moral reasoning: The Theory of Cognitive Moral Development and the Theory of Motivational Types of Values (Kohlberg, 1984; Schwartz, 2007).

Meanwhile, some information security research has focused on whether information security awareness actually impacts information security. For instance, Siponen (2000) finds that the accepted notion of information security awareness, as a descriptive construct, is not sufficient for explaining factual, i.e. normative, aspects of information security. He further

argues that motivation, as a recognized precursor for action, is not sufficiently considered in terms of information security. In order to reconcile this problem, Siponen states that all user behavior that is thought to have an impact upon information security should satisfy the requirements of behavioral theories and provide answers to end-users about why they should consider information security in their daily actions. Using this criteria, Siponen further states that arguments based on morals and ethics, such as those cited above, should be discarded.

In 1992, researchers looked at twelve specific threats and identified their relative rankings in a survey of MIS executives in terms of three distinct computing environments; microcomputer, mainframe, and networking (Loch, Carr, & Warkentin, 1992). They found that threats to organizations' information security could arise from inside the organization as well as from outside the organization. This marked another milestone in the cognitive shift from thinking of information security in terms of just physical security, where only a few administrators had access to isolated mainframe computers, to data security where it is necessary for IT administrators to safeguard networked information assets. As evidence of this shift the researchers noted that computer viruses posed a growing threat to information security and, as such, included it in their survey. The concept of the computer virus had previously been described by J.A. Schweitzer (1989) and Davis and Gantenbein (1987). By the early 1990s, the concept of the computer virus was already beginning to gain recognition in the information systems literature as a viable information security threat.

Loch, Carr & Warkentin's results indicated that a greater percentage of the respondents surveyed perceived the risk of computer disruption to be higher in the microcomputer environment (56%), as compared to the mainframe environment, where 62% of the respondents classified the risk of computer disruption to be low (Loch, Carr, & Warkentin, 1992). Computer

viruses were ranked as the fourth most important threat in the network environment and sixth overall in the microcomputer environment. An interesting ancillary finding of this study, which has significant implications for the present research, was that the "Education and Training" industry together with "Information Services" and "Manufacturing" comprised 68% of the reported verified incidences of computer viruses. Of those three categories, by far the largest was the "Education and Training" industry, accounting for 60% of verified incidents of a computer virus (Loch, Carr, & Warkentin, 1992).

2.5 Information Security Research in Higher Education Environments

It was not until much later, however, that scholarly articles began to explore information security within the context of institutions of higher learning. One article to do so explored information security readiness in higher education from the vantage point of a state-sponsored university in a developing country (Rezgui & Marks, 2008). The authors of that article adopted a case study approach to identify the political, social, and cultural factors that adversely affected information security awareness at Zayed University in the United Arab Emirates. While many of the authors' conclusions are not applicable to a domestic view of institutions of higher learning because of strong cultural and organizational differences, it is a premise of this dissertation that the lack of transparency between departments, as well as complacency in monitoring behaviors, which Rezgui and Marks identify in their research, are also present in institutions of higher learning located in the United States. In support of this observation, an EDUCAUSE study (Updegrove & Wishon, 2003) highlighted an apparent cybersecurity readiness gap in 435 higher education institutions surveyed. This gap was made apparent by yet another article, which asserted that a third of higher education institutions experienced a data loss or theft during 2006,

with nine percent of those reporting a loss or theft of confidential student information (Piazza, 2006).

Cybersecurity incidents at the University of Maryland and at the North Dakota University system in 2014 underscore the fact that universities are not immune to cyberattack. The first incident, involving one of the University of Maryland's primary databases, resulted in the unauthorized exposure of more than 390,000 student and staff records. The North Dakota University system experienced a similar data breach in which over 290 student and staff records were compromised (Ponemon Institute, L.L.C., 2014). Such data breaches occurred even though, according to the Updegrove and Wishon article, 92% of institutions they surveyed indicated that they had an institutional ISP in place at the time of the attack. A far more troubling insight from that article is that a bare majority of respondents indicated using known best practices. For instance, only 57% of the respondents in their survey reported having a password change policy that was ninety days or less. A relative minority, 39%, of the schools surveyed, indicated the presence of an IS awareness program in their institutions and only 30% reported using risk assessment and audit procedures (Updegrove & Wishon, 2003).

Clearly, more can be done at the institutional level to safeguard the information resources of colleges and universities. The situation is further complicated by the decentralized levels of IT administration at institutions of higher learning, which due to limited budgets and limited staff, may not be as prepared in terms of cybersecurity readiness as centralized, institution-wide IT departments. The question remains then, how does the cybersecurity readiness picture at the decentralized department level in complex, multi-tiered organizations such as colleges and universities look? Furthermore, what can be done at the organizational-unit level of such institutions to safeguard valuable information resources?

2.6 Defense in Depth Strategy

A potential answer to the questions listed above appears in an article from the September/October 2000 issue of *IEEE Software*. The authors of that article argue that in addition to normal preventative measures such as formulating a security policy, creating user authentication and access control lists, creating strong password requirements, and eliminating unnecessary services, individual network administrators should introduce an intrusion detection component into their network schema, as one aspect of what the authors refer to as, "defense in depth" (McHugh, Christie, & Allen, 2000). Defense in depth consists, in part, of network sensors outside of the protected network, which allow the administrator to gain a sense for the general threat level around a system's periphery, as indicated by probes and attempts that are detected that otherwise would have been blocked by the firewall. As the authors state, a defensive posture that employs network sensors on both sides of the firewall allows the administrator to validate and correctly configure firewall rules.

However, a "Defense in Depth" strategy may be beyond the financial and technical capabilities of individual departments, which are often forced to operate with limited staff and small budgets. Furthermore, IT administrators who are employed outside of the institution's centralized IT department often have their ability to effect changes like firewall configurations restricted by official institution policy. Many times, such responsibilities reside solely with the institution's centralized IT department. It is the premise of this dissertation, therefore, that a "Defense in Depth" strategy often is not feasible at the organizational-unit level of IT administration in complex, multi-tiered organizations. Therefore, a different strategy is needed. The proposed strategy should not solely rely on technological solutions, such as those that McHugh et al. propose, since such solutions are costly both in terms of purchasing and

implementation. Rather, it will be far more effective to leverage existing resources to increase cybersecurity readiness. One such resource, which many organizational units have, is a human resource in the form of one or more workgroup IT managers.

To increase the cybersecurity readiness of such administrators, and by extension increase the cybersecurity readiness of the organizational unit, it is first necessary to get a baseline measure for the current state of cybersecurity readiness at this level of administration. However, in the absence of reliable data that shows the type, frequency, and severity of cyberattacks against specific organizational units, such as departments and schools at institutions of higher learning, information security researchers must adopt an adequate proxy. An IT manager's perception of his or her cybersecurity readiness can serve as an adequate proxy for his or her actual cybersecurity readiness, in much the same way that an individual's perceived capability for managing his or her health outcomes has been shown to correlate strongly with his or her actual intentions to manage personal health outcomes, as demonstrated by instruments like the Perceived Health Competence Scale (PHCS) (Smith, Wallston, & Smith, 1995). This view is substantiated, in large part, because of the theoretical justifications of self-efficacy theory (SET), as laid out by Albert Bandura in his 1977 treatise, "Self-efficacy: towards a unifying theory of behavioral change."

2.7 Previous Experience with Cybersecurity

In their article, McHugh et al. raise the valid point that cyberattacks involve multiple perspectives (2000). They state that the administrator, whose responsibility it is to safeguard the information technology resources of the organizational unit, should be concerned with answering questions such as, who was affected by a cyberattack, why did it happen, what happened, and when and where did the intrusion occur? The attacker, on the other hand, is concerned with

questions that revolve around his or her objective and its associated risk. Such questions may pertain to the nature of the objective, the nature of any vulnerabilities that exist, the amount of damage the attack is likely to result in, the nature and severity of any consequences that may result from the action, and the availability and applicability of existing exploit scripts or attack tools. The ability to conceptualize of a cyberattack from both viewpoints is therefore pertinent to a broader understanding of perceptions of cybersecurity readiness. As discussed later in Chapter 3, both viewpoints are incorporated into the PACRM model as part of the *Level of Previous Experience with Cybersecurity* construct, a summative measure that is comprised of the hours spent in cyber threat detection and prevention training, and his or her self-reported level of experience with stopping and initiating cyberattacks.

2.8 Information Security: The Quest for the Dependent Variable

The quest for a dependent variable in information security research is an ongoing process. In many respects, the process is complicated by the seemingly straightforward nature of information security. The goal of such research is, after all, to improve information security within organizations by either preventing cyberattacks or otherwise mitigating their adverse effects. Information security, therefore, does seem to be the logical choice as a dependent variable and indeed, many recent research studies have adopted information security as their response variable of choice (Sapegin, et al., 2017). However, what does information security entail? Widely accepted notions of information security emphasize that information should be confidential, available, and authentic (Whitman & Mattord, 2016). Therefore, one possible definition of information security is the process by which these characteristics of an organization's information resources are safeguarded from unauthorized manipulation. To achieve that goal, however, it is necessary for IT managers to engage in concrete activities

related to safeguarding the availability, authenticity, and confidentiality of their organization's information resources. It is the premise of this dissertation that these activities are predicated on the IT manager's ability to detect, prevent, and, if necessary, recover from a cyberattack.

2.9 Security Information and Event Management

Security Event Management (SEM) and Security Information Management (SIM) are two aspects of Security Information and Event Management (SIEM), which relies on real-time monitoring and correlation of events to gauge security threats. The monitoring of real time data events through the collection of log data is part of SEM, while the long-term storage and statistical analysis of log data is an aspect of SIM. Not surprisingly, SIEM consists of data aggregation from multiple sources including network devices, security sensors, servers, and databases. SIEM is incorporated into the PACRM model in Chapter 3 as the *Extent of the IT Manager's Use of Network Monitoring Mechanisms* factor.

2.10 Cybersecurity Best Practice Frameworks

The Center for Internet Security (CIS) lists 20 top controls for managers to use in securing their information systems' infrastructure (CIS Controls, 2017). Among other items, included in that list are: Secured configurations for hardware and software, controlled use of administrative privileges, maintenance, monitoring, and analysis of audit logs, malware defenses, data recovery capabilities, boundary defense, controlled access based on the need to know, account monitoring and control, and security skills assessment and appropriate training to fill the gaps (CIS Controls, 2017). Each of the controls listed above is represented by elements of the PACRM model, discussed in Chapter 3.

Table 1 presents a brief synopsis of the elements associated with the *Extent of Use of Cybersecurity Best Practices* and the *Degree of User Community Awareness of Security Issues* factors from the PACRM model and their corollaries among the CIS controls.

Table 1: PACRM Elements and their CIS Control Corollaries

PACRM Model Element		**CIS Controls Description** (Center for Internet Security, 2017)
Use and Routinely Monitor Network Activity Logs		Collect, manage, and analyze audit logs of events that could help detect, understand, or recover from an attack.
Employ Intrusion Detection Systems (IDS) and/or Intrusion Prevention Systems (IPS) and sensor deployments and/or traffic analyzers		Detect/prevent/correct the flow of information transferring networks of different trust levels with a focus on security-damaging data.
Control unauthorized physical access to network and server resources through physical means or electronic means such as locking the BIOS or encryption		The processes and tools used to track/control/prevent/correct secure access to critical assets (e.g., information, resources, systems) according to the formal determination of which persons, computers, and applications have a need and right to access these critical assets based on an approved classification.
Require Strong Passwords and Require Users to Update Passwords		Actively manage the life cycle of system and application accounts – their creation, use, dormancy, deletion – to minimize opportunities for attackers to leverage them.
Run Critical Operating System or Application Software Updates		Manage the security life cycle of all in-house developed and acquired software to prevent, detect, and correct security weaknesses.
Perform Regular System Backups with Backups that are Stored Offline		The processes and tools used to properly back up critical information with a proven methodology for timely recovery of it.
Ensure User Community Awareness on Security Issues		For all functional roles in the organization (prioritizing those mission-critical to the business and its security), identify the specific knowledge, skills, and abilities needed to support defense of the enterprise; develop and execute an integrated plan to assess, identify gaps, and remediate through policy, organizational planning, training, and awareness programs.

In addition to the Center for Internet Security guidelines listed above, there is a wide range of frameworks that provide guidelines for cybersecurity best practices. Three of the most widely used of these frameworks are the NIST 800-14 (Swanson & Guttman, 1996), the ISO 27000 series (International Standards Organization, 2017), and the NIST 2014 framework for improving critical cybersecurity infrastructure (NIST, 2014).

While the NIST 800-14 framework identifies many controls related to information security, Chapter 3 of the NIST standard is particularly relevant because it pertains to IT security practices. Specifically, the sections that are most pertinent to the present discussion are personnel/user issues (3.5), computer security incident handling (3.7), awareness and training (3.8), security considerations in computer support and operations (3.9), and physical and environmental security (3.10). Each of these chapter sections contain controls that are reflected in the PACRM model, discussed in Chapter 3 of this dissertation. For example, section 3.7 in the NIST framework contains controls for an "Educated Constituency," which is reflected in the *Degree of User Community Awareness of Security Issues* factor of the PACRM model. Likewise, section 3.9 contains controls for software support, which includes controls for periodic backups and regular application backups. These items are reflected in the PACRM model as the *Extent of Use of Preventative Software Measures* and *Extent of Use of a Backup Policy where Backups are Kept Offline* factors. Since 1996, the NIST 800-14 framework has directed U.S. federal government efforts in terms of information security.

Conversely, the ISO 27000 series of cybersecurity guidelines are directed towards improving cybersecurity in organizations all over the world. The ISO 27000 framework is a series of related guidelines, which IT managers across a wide range of domains and organizations can use to strengthen and refine their cybersecurity strategies. As such, it was not

written to be directly applicable to government settings. It does, however, share many controls in common with frameworks that were. For example, ISO 27002, which was originally published in October 2005, contains controls for human resources security as well as access control and operations security. Both controls closely mirror the NIST 800-14 elements listed above.

Finally, the NIST 2014 framework represents the latest iteration in the evolution of information and cybersecurity best practices. Each of the core categories in the framework are aligned with five high-level functions. These functions are: Identify, Protect, Detect, Respond and Recover (NIST, 2014). Three of these five functions are represented as the response variables of choice in the PACRM model presented in Chapter 3 of this dissertation. Table 2 presents the brief descriptions of the high-level NIST functions, as articulated by the framework.

Table 2: NIST 2014 Framework for Improving Critical Cybersecurity Infrastructure High-Level Function Descriptions

NIST 2014 High-Level Function		**Description** (NIST, 2014)
Identify		Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.
Protect		Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.
Detect		Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.
Respond		Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.
Recover		Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.

These descriptions illustrate that, of the five functions enumerated, only four are directly applicable to the organizational-unit level. The function that does not directly pertain to specific,

organizational-unit level activities is the Identify function. The Identify function is primarily concerned with orienting the organization's policy towards an awareness of information security issues. As such, it is more suitable to levels of IT administration above that of the individual, organizational unit, which forms the unit of analysis for the present discussion. The Response and Protect functions, meanwhile, are closely related. The primary difference between the two functions is that the Response function is concerned with communications, analysis, and response management after a cyberattack has occurred. It is unlikely that individual workgroup IT managers, who work at the decentralized level of IT administration will have a codified response management plan, complete with mitigation strategies and communication protocols. This is deemed to be particularly true in institutions of higher learning where the IT personnel of any one school or department often labor under reduced staff and budgetary considerations. It may be useful, however, to test this assumption in future iterations of the PACRM model in larger organizational units where the specific strategies of the response function are more likely to be utilized.

2.11 Self-Efficacy

Figure 3 is taken from Albert Bandura's initial paper on self-efficacy. In that paper, Bandura differentiates between outcome expectations and efficacy expectations in the following manner. Outcome expectations are those expectations that cause an individual to estimate that a given set of behaviors will result in a certain outcome. Efficacy expectations, on the other hand, are the individual's belief that he or she can successfully execute the set of behaviors required to produce the desired outcome.

Figure 3: Diagrammatic representation of the difference between efficacy expectations and outcome expectations (Bandura, 1977).

For instance, an individual may reasonably expect that a certain behavior, or set of behaviors, will lead to a given outcome based on previous empirical or academic knowledge. At the same time, however, he or she may be reasonably uncertain as to whether they can enact such behavior(s). Efficacy expectations affect both an individual's initial coping behaviors and the persistence of those coping behaviors in the face of challenges. Given that the appropriate skills and effective incentives are present, an individual's efficacy expectations are a strong determinant of his or her choice of activities, how much effort he or she will expend in the pursuit of a goal, and how long he or she will sustain effort in the face of challenges towards that goal (Bandura, 1977).

We might reasonably substitute the components of information security discussed above into Bandura's original model, as illustrated below in Figure 4. By doing so, we see that a workgroup IT manager's actual ability to detect, prevent, and recover from a cyberattack are outcome expectations, while his or her perceived readiness to perform those same actions are efficacy expectations. That is, in Bandura's original conceptualization, by increasing his or her abilities with respect to detection, prevention, and recovery of cyberattacks, an IT manager may reasonably expect to suffer fewer and/or less severe cyberattacks, relative to the ultimate outcome of such attacks. However, his or her perceived readiness to detect, prevent, and, if necessary, recover from a cyberattack translates into a belief as to whether he or she can perform

those behaviors. Since the IT manager at this level of administration is integral to determining the cybersecurity readiness of the organizational unit, it stands to reason that the organizational unit likewise benefits from an increase in either the manager's outcome expectations or in his or her efficacy expectations.

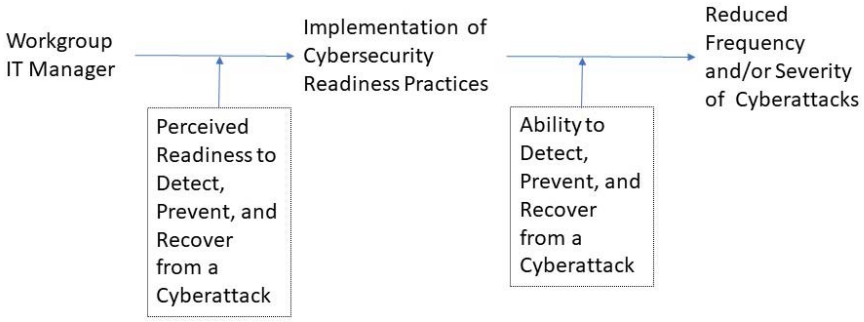

Figure 4: Self-efficacy theory (SET) model with information security components

While it is instructive to situate elements of information security within Bandura's original framework to show that self-efficacy is germane to the present discussion, this dissertation is not concerned with merely validating Bandura's original SET model in a new context, any more than has already been done. SET has already been applied to the information and computer domain through previous research, most notably in the form of Computer Self-Efficacy (CSE) (Compeau & Higgins, 1995).

3 THEORETICAL CONTRIBUTIONS

3.1 Research Questions

The present dissertation is concerned with answering the following questions.

RQ1: What factors are associated with the perceived readiness of workgroup IT managers to detect, prevent, and if necessary, recover from a cyberattack?

RQ2: Does attitude towards risk affect the relationship between an IT manager's previous level of experience and the extent of his or her use of cybersecurity best practices.

To attempt to answer these questions, we start by revisiting Bandura's original definition of efficacy expectations. Recall that efficacy expectations are an individual's belief in his or her ability to produce a given set of behaviors. In terms of information security management, efficacy expectations represent the IT manager's perceived readiness to detect, prevent, and recover from a cyberattack. These perceptions, in turn, affect his or her actual cybersecurity readiness.

As per Bandura's original (1977) model, efficacy expectations are informed by four major sources of information. Among these are performance accomplishments, vicarious experiences, verbal persuasion, and emotional arousal. Each of these four sources of information provide feedback to the participant, which helps to strengthen his or her efficacy expectations. Each of the four sources, in turn, can be supplied through different modes of induction. Figure 5 is from Bandura's article and helps to illustrate the portion of his model pertaining to efficacy

expectations. Figure 6 is a repeat of Figure 1 from this dissertation. It illustrates the PACRM model in its entirety. It has been placed below for the convenience of the reader.

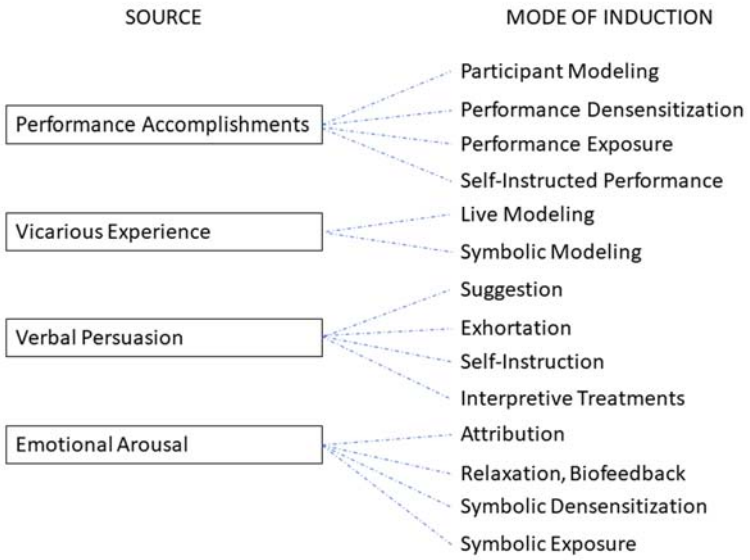

Figure 5: Efficacy Expectations (Bandura, 1977)

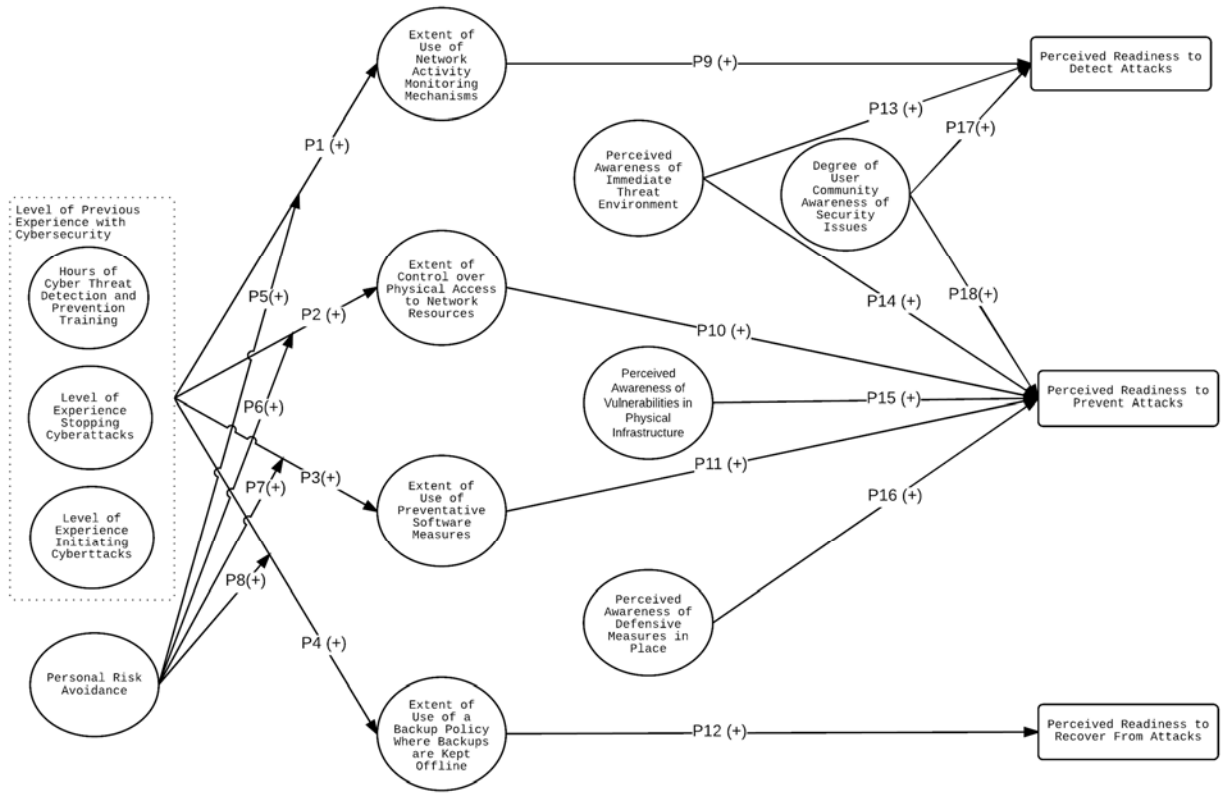

Figure 6: PACRM Conceptual Model Diagram (Repeat of Figure 1)

The PACRM model, shown in Figure 6 above, incorporates several of Bandura's original sources that are believed to affect an IT manager's perceived readiness to detect, prevent, and recover from a cyberattack. Recall that the four primary factors of the PACRM model are the IT manager's previous level of cybersecurity experience, the extent of his or her use of cybersecurity best practices, his or her awareness of the computer and network environment in and around the organizational unit, and the degree to which the user community that he or she supports is educated about issues related to information security. Recall, also, that the secondary research questions that are pertinent to this research are:

RQ1a: How is an IT manager's previous level of cybersecurity experience related to his or her perceived readiness to detect, prevent, and recover from a cyberattack.

RQ1b: How is the extent of an IT manager's use of cybersecurity best practices related to his or her perceived readiness to detect, prevent, and recover from a cyberattack.

RQ1c: How is an IT manager's awareness of the computer and network environment in and around the organizational unit related to his or her perceived readiness to detect and prevent a cyberattack.

RQ1d: How is the degree to which the user community is educated about issues pertaining to information security related to the IT manager's perceived readiness to detect and prevent a cyberattack.

It can be surmised that the factors related to research question 1c use the modes of induction related to the emotional arousal source from Figure 5 above. In other words, an IT manager's level of awareness of his or her environment entails, by its nature, a level of comfort (or discomfort) with various aspects of that environment. Similarly, since previous training and experience with cybersecurity-related activities entails a degree of real-world and simulated events, it stands to reason that the factor of the PACRM model that is related to a manager's previous level of cybersecurity experience necessarily incorporates aspects of both the performance accomplishments and vicarious experience sources, together with their concomitant modes of induction.

In Bandura's original research, he surmises that the performance accomplishment and vicarious experience sources are both thought to exert a stronger influence over an individual's efficacy expectations than does the emotional arousal source. For that reason, we might expect to see a relatively strong correlation between an IT manager's previous level of experience with cybersecurity and his or her perceived readiness to detect, prevent, and recover from a cyberattack. However, that relationship will be somewhat mediated by the extent to which he or she uses known cybersecurity best practices.

3.2 Conceptual Model Description

The argument that theory is an important component in confirmatory research is well established in the psychometric literature (Blalock, 1969; Bagozzi, 1980). The use of theories to

drive confirmatory research works because they help to pre-specify the nature of constructs, which in turn informs the measurement of those constructs. In addition, the use of well-grounded and clearly articulated theories propels research within a given domain by providing a firm foundation upon which to build future research. Theory also aids in the clear specification of measurements, thereby strengthening the conclusions garnered by those measurments (Churchill, 1979).

Figure 6 shows that the factors for the model are organized into four main groups. The first group is the IT manager's level of previous experience with cybersecurity. It attempts to answer *RQ1a* from above. The second group of factors attempts to capture the extent to which the manager uses cybersecurity best practices. In doing so, it seeks to answer *RQ1b*. The third group is a set of awareness-based factors that are related to *RQ1c*. The factors that comprise this group attempt to capture the manager's level of knowledge and awareness with various aspects of his or her computer and network environment. The fourth group, relevant to *RQ1d*, is made up of a single factor that looks at the degree to which the user community that the IT manager supports is educated about issues related to information and computer security. Lastly, the IT manager's risk avoidance score on a group of variables serves as a moderator of the relationships between the IT manager's *Level of Previous Experience with Cybersecurity* and the *Extent of Use of Cybersecurity Best Practices* factors.

Together, these factors are thought to inform the IT manager's perceived readiness to detect, prevent, and, if necessary, recover from a cyberattack. Table 3 lists the factors shown in Figure 6, along with a short description of each.

Table 3: PACRM Factors and Descriptions of Their Associated Survey Elements

PACRM Model Factor		**Factor Description**
Hours of Cyber Threat Detection and Prevention Training		The total amount of time that the IT manager has spent engaged in cyber threat detection

		and prevention training. This variable may include the time spent in formalized training programs and/or spent preparing to obtain cybersecurity related certifications. Part of the summative factor, *Level of Previous Experience with Cybersecurity*.
Level of Experience Stopping Cyberattacks		The level of self-reported experience with stopping cyberattacks. The IT manager may have obtained such experience through training programs or through on-the-job cybersecurity tasks, such as working as an independent Certified Ethical Hacker© or as a security specialist. Part of the summative factor, *Level of Previous Experience with Cybersecurity*.
Level of Experience Initiating Cyberattacks		The level of self-reported experience with initiating cyberattacks. As with *Level of Experience Stopping Cyberattacks*, the IT manager may have gathered such experience through formalized training sessions, certification programs, or actual hacking experience. Part of the summative factor, *Level of Previous Experience with Cybersecurity*.
Personal Risk Avoidance Score		Attempts to capture the IT Manager's attitudes toward risk avoidance in both general terms and in terms of workplace information security.
Extent of Use of Network Activity Monitoring Mechanisms		The extent of the IT manager's use of network activity logging mechanisms such as IDS/IPS and sensor deployments and/or traffic analyzers to capture actual network events. Utilization of network activity monitoring measures also implies the periodic and systematic review of activity logs to look for signs of suspicious activity or adverse events.
Extent of Control Over Physical Access to Network Resources		The extent of the IT manager's level of control over physical access to computer and

		network resources within his or her school or department. Restricting physical access can be achieved through a combination of physical deterrents (such as locked rooms and/or server cabinets) or electronic means (such as by locking the BIOS or using encryption).
Extent of Use of Preventative Software Measures		The extent of the IT manager's use of preventative measures as part of his or her computer security strategy.
Extent of Use of a Backup Policy Where Backups are Kept Offline		The extent to the which the IT manager uses regular backup processes as part of a working backup policy of business-critical computer resources.
Perceived Awareness of the Immediate Threat Environment		The IT manager's level of knowledge about the volume, type, and integrity of network traffic, which exists on the computer network that he or she supports. This measure also attempts to capture the IT manager's level of awareness that the computers he or she supports are free from viruses or malware and are not being used in the support of illicit activities, such as in support of a Distributed Denial of Service (DDoS) attack.
Perceived Awareness of Vulnerabilities in the Physical Infrastructure		The IT manager's level of knowledge about the physical infrastructure of his or her computer network as well as any potential vulnerabilities that may exist. The IT manager's level of awareness of the number of potential vulnerabilities in his or her computer network as well as the physical infrastructure of his or her computer network.
Perceived Awareness of Defensive Measures in Place		The IT manager's level of knowledge about the type of defensive measures currently in place to protect his or her computer network from unauthorized access. The IT manager's level of awareness of the type of defensive measures that are in place to secure his or her computer network.

Degree of User Community Awareness of Security Issues		The degree to which the end user community that the IT manager supports is educated on, and aware of, several issues related to computer and information security.

3.3 Research Propositions

The four groups of factors, as mentioned above, are the IT manager's previous level of experience with cybersecurity, the extent of his or her use of cybersecurity best practices, his or her awareness of various aspects of the computer and information environment in and around the organizational unit, and the degree to which the user community that he or she supports is educated and aware of issues pertaining to security.

The first factor is a simple composite measure, comprised of the amount of time that the IT manager has spent engaged in cyberattack detection and prevention training, either as a part of a certification program or otherwise. Also included in this factor is the manager's self-reported level of previous experience with stopping cyberattacks and his or her self-reported level of previous experience with initiating cyberattacks. Each of these activities may legitimately be performed as one aspect of a training program or during work which is lawfully performed as a security analyst. The IT manager's overall level of previous cybersecurity experience is proposed to have a positive relationship with each of the four factors associated with the *Extent of Use of Cybersecurity Best Practices* factors. These relationships can be seen in Figure 6 above. As a manager's overall level of previous experience in cybersecurity increases, the extent of his or her use of best practices should likewise increase. The decision to make the IT manager's *Level of Previous Experience with Cybersecurity* a summative measure was made early in the conceptual design process. It was thought that, due to the sensitive nature of asking professionals to voluntarily divulge the relative frequency that they have spent initiating cyberattacks, that a

probable floor effect would be seen in that variable. Therefore, the decision was made to make it part of a summative construct to help mitigate that possible effect.

The proposed relationships between the IT manager's *Level of Previous Cybersecurity Experience* and his or her *Extent of Use of Cybersecurity Best Practices* are moderated by his or her level of *Personal Risk Avoidance*. Therefore, the relationship between an individual's previous experience with cybersecurity and the extent of that individual's use of cybersecurity best practices should be more pronounced for those individuals with a higher level of risk avoidance.

The extent of an IT manager's use of best practices contains four factors. These factors attempt to capture information about the extent of the IT manager's use of network activity monitoring mechanisms, the extent to which the IT manager exercises physical control to computer and network resources, the extent of the IT manager's use of preventative measures such as firewalls and strong passwords, and the extent of the IT manager's use of a backup policy with backups that are kept offline. Each of these factors are proposed to be related to the perceived readiness factors in the following ways.

First, the *Extent of the Use of Network Activity Monitoring Mechanisms* factor examines the degree to which the IT manager uses activity logging mechanisms such as IDS/IPS deployments and/or sensor deployments to capture and log real-time network events. This factor also measures whether log data, if it is captured, undergoes a systematic review to search for signs of adverse events or suspicious activity. This factor is therefore proposed to have a positive relationship with the manager's *Perceived Readiness to Detect Attacks*. The reasoning behind this proposed relationship is that an IT manager should find him or herself in a more

advantageous position to detect a cyberattack if he or she is periodically willing and able to capture and review network activity log data.

The second factor in this group is the *Extent of Control Over Physical Access to Network Resources* factor. Restricting physical access to sensitive computer and network resources has been shown to be effective in reducing incidents of computer abuse. The relationship between this factor and the manager's *Perceived Readiness to Prevent Attacks* is therefore proposed to be a positive one.

Third, the *Extent of Use of Preventative Software Measures* factor is likewise thought be positively related to the *Perceived Readiness to Prevent Attacks* factor. Preventative software measures include the use of strong passwords to authenticate users as well as the use of antivirus and anti-malware software to check for malicious software on the computer. In addition, software-defined firewalls prevent unauthorized intrusions that originate from outside the computer. Regular critical software and operating system updates are also thought to contribute to this factor.

Finally, the *Extent of Use of a Backup Policy Where Backups are Kept Offline* factor is thought to have a positive relationship to *Perceived Readiness to Recover from an Attack*. This proposed relationship is based on the reasoning that offline backups can be used to preserve clean copies of the organizational unit's data, which can then be used to recover services in the event of a malicious attack. Since hackers often target online backups to manipulate them in the same manner as they have done with the primary system, the offline component of this factor is deemed to be especially important component of this factor.

The perceived awareness factors consist of three general elements. First, *Perceived Awareness of the Immediate Threat Environment* attempts to capture the level of knowledge and

awareness that the IT manager has about the volume, type, and integrity of network traffic on both the network that he or she supports and any intersecting networks. This factor is proposed to have direct, positive relationships with both *Perceived Readiness to Detect Attacks*, and *Perceived Readiness to Prevent Attacks*. Therefore, the greater the manager's awareness of the threat environment, i.e. the more comfortable he or she feels about the state of knowledge about the status of the computer network, then the greater the readiness he or she should feel to detect and prevent any potential cyberattacks against that network.

The second factor in the awareness-based group is the *Perceived Awareness of Vulnerabilities in the Physical Infrastructure* factor. This factor attempts to capture whether the IT manager is knowledgeable about both the physical infrastructure of the organizational unit's computer network and any potential vulnerabilities within that infrastructure. This factor is thought to have a positive relationship with *Perceived Readiness to Prevent Attacks*. As a manager's level of knowledge and awareness about the physical infrastructure of the computer network increases, so too will his or her perceived readiness to prevent a potential cyberattack.

The final factor in the awareness-based group is *Perceived Awareness of Defensive Measures in Plac*e. The term "defensive measures" is left vague by design. Such measures may be procedural (sign-in sheets to access sensitive computer or data resources, etc.), physical (restricted physical access, separate subnets and physical connections for sensitive resources, etc.), or electronic (firewalls, IPSs, etc.). Rather than list all, or even a subset, of the possible defensive measures, it was instead determined that the purpose of this factor is to capture the IT manager's level of knowledge and awareness of whatever defensive measures he or she has in place. This factor is proposed to positively affect *Perceived Readiness to Prevent Attacks*. As

the manager's level of knowledge and awareness of his or her defenses increases, so too should his or her perceived readiness to prevent cyberattacks.

Finally, the *Degree of User Community Awareness About Issues Pertaining to Security* factor is thought to be positively related to both *Perceived Readiness to Detect Attacks* and *Perceived Readiness to Prevent Attacks*. Several of the IT managers who were interviewed during the initial pilot testing phase of the project remarked that their readiness to detect and prevent cyberattacks is largely dependent on their users. It was therefore determined that the awareness of an organizational unit's user community on various issues related to computer and information security could be a vital component in determining the IT manager's perceived readiness to detect and prevent cyberattacks. Aspects of user community awareness may include the need to keep computer operating systems and applications consistently updated, the need to exercise caution when bringing external USB drives and storage devices into the workplace, the need to exercise caution when downloading and installing software from the Internet, the need to exercise caution when confronting communication situations that could potentially divulge sensitive information to unauthorized personnel, and the need to exercise caution when opening email attachments or clickable links. Table 4 lists the proposition number, as illustrated in Figure 6 presented above, along with a short description of each.

Table 4: PACRM Propositions and Their Associated Descriptions

PACRM Proposition Number		**Proposition Description**
1		The IT manager's level of previous experience with cybersecurity is positively related to the extent of his or her use of network activity monitoring mechanisms.
2		The IT manager's level of previous experience with cybersecurity is positively related to the extent of his or her control over unauthorized physical access to computer or network resources within the school or department.

3		The IT manager's level of previous experience with cybersecurity is positively related to the extent of his or her use of preventative software measures.
4		The IT manager's level of previous experience with cybersecurity is positively related to the extent of his or her use of a backup policy where the backups are kept offline.
5		The extent of the IT manager's use of network activity monitoring mechanisms will be greater for those managers who show a greater level of risk avoidance then it will be for managers who are less risk avoidant, holding previous level of cybersecurity experience constant.
6		The extent of the IT manager's control over physical access to the computer network will be greater for those managers who show a greater level of risk avoidance, then it will be for managers who are less risk avoidant, holding previous level of cybersecurity experience constant.
7		The extent of the IT manager's use of software preventative measures will be greater for those managers who show a greater level of risk avoidance, then it will be for managers who are less risk avoidant, holding previous level of cybersecurity experience constant.
8		The extent of the IT manager's use of a backup policy where backups are kept offline will be greater for those managers who show a greater level of risk avoidance, then it will be for managers who are less risk avoidant, holding previous level of cybersecurity experience constant.
9		The extent to which the IT manager uses network activity monitoring mechanisms is positively related to his or her perceived readiness to detect cyberattacks.
10		The extent to which the IT manager controls physical access to network resources is positively related to his or her perceived readiness to prevent cyberattacks.
11		The extent to which the IT manager uses preventative software measures is positively related to his or her perceived readiness to prevent cyberattacks.
12		The extent to which the IT manager uses a backup policy where the backups are kept offline is positively related to his or her perceived readiness to recover from a cyberattack.
13		The IT manger's perceived awareness of the immediate threat environment in and around his or her organizational unit is positively related to his or her perceived readiness to detect a cyberattack.
14		The IT manager's perceived awareness of the immediate threat environment in and around his or her organizational unit is positively related to his or her perceived readiness to prevent a cyberattack.
15		The IT manager's perceived awareness of vulnerabilities in the physical infrastructure he or she supports is positively related to his or her perceived readiness to prevent a cyberattack.
16		The IT manager's perceived awareness of defensive measures in place is positively related with his or her perceived readiness to prevent a cyberattack.

17		The degree of user community awareness of security issues is positively related with the IT manager's perceived readiness to detect a cyberattack.

4 METHODOLOGY

4.1 PACRM Measurement Model

Each of the conceptual factors listed above have their associated elements in the PACRM survey, which is presented in its initial iteration in Appendix B and in its final version as Appendix C. For the convenience of the reader, Table 5 presents the full measurment model detailing how each factor is to be measured.

Table 5: PACRM Measurement Model

Concept	Construct	Survey Items	Description
Previous Experience	Level of Previous Experience with Cybersecurity	PE.3 PE.4.1 PE.4.2	• Number of hours spent taking part in cybersecurity training. • Previous level of experience with preventing or stopping cyberattacks. • Previous level of experience initiating cyberattacks.
Risk Avoidance	Personal Risk Avoidance Score	D.8.1 D.8.2 D.8.3	• General risk avoidance • Risk avoidance in work settings. • Risk avoidance in terms of information security at work.
Network Activity Monitoring	Extent of Use of Network Activity Monitoring Mechanisms	EU.1.1 EU.1.2 EU.1.3 EU.2.1 EU2.2 EU2.3	• Extent of Use of and frequency checking network activity logs to monitor network activity. • Extent of Use of and frequency monitoring IDS and /or IPS reports on the network. • Extent of Use of and frequency analyzing sensor deployment and/or traffic analyzer reports for the network.

Physical Access Control	Extent of Control over Physical Access to Network Resources	EU.1.4 EU.1.5 EU.1.6 EU.2.4	• Extent of use of controlling physical access to network and server resources. • Servers or other vital computer resources are secured in a locked room or server cabinet. • Extent of use of computers with a locked BIOS where it is impossible to boot from an external device.
Preventative Measures	Extent of Use of Preventative Software Measures	EU.1.7 EU.1.8 EU.1.9 EU1.10 EU1.11 EU1.12 EU.2.5 EU.2.6 EU.2.7 EU.2.8 EU.2.9 EU.2.10	• Computers with encrypted hard drives. • Servers or other vital computer resources with encrypted hard drives. • Strong passwords updated regularly to prevent unauthorized use. • Computers protected with antivirus software that is updated regularly. • Computers protected with anti-malware software that is updated regularly. • Computers protected by one or more firewalls with settings updated to reflect current and emerging threats and to allow for approved applications. • Critical software and operating system updates.
Regular Offline Backups	Extent of Use of a Backup Policy Where Backups are Kept Offline	EU.1.13 EU.2.11	• Regular backups of servers or other vital computer resources that are then kept offline.
User Community Awareness	Degree of User Community Awareness of Security Issues	ED.1.1 ED.1.2 ED.1.3 ED.1.4 ED.1.5 ED.1.6	• Users are educated about the need to update work computer operating system and/or applications regularly. • Users are educated about the need to update work computer antivirus definitions regularly. • Users are educated about the need to exercise caution when using an external USB drive.

			• Users are educated about the need to exercise caution when downloading and installing software or apps from untrusted sources. • Users are educated about the need to exercise caution when engaging in conversations about sensitive information. • Users are educated about the need to exercise caution when opening email attachments and clickable links in email.
IT Manager Awareness of Threat Environment	Perceived Awareness of Immediate Threat Environment	PA.1.1 PA.1.2 PA.2.1 PA.2.2	• Level of knowledge and awareness about the volume and type of network traffic flowing through the network. • Level of knowledge and awareness about the integrity of network traffic on intersecting networks.
IT Manager Awareness of Physical Infrastructure	Perceived Awareness of Vulnerabilities in Physical Infrastructure	PA.1.3 PA.1.4 PA.2.3 PA.2.4	• Level of knowledge and awareness about the physical infrastructure of the network. • Level of knowledge and awareness about potential vulnerabilities within the network.
IT Manager Awareness of Defensive Measures in Place	Perceived Awareness of Defensive Measures in Place	PA.1.5 PA.2.5	• Level of knowledge and awareness about type of defensive measures in place.
Readiness to Detect Attacks	Perceived Readiness to Detect Attacks	PR.1.1 PR.1.2 PR.2.1	• Perceived ability and readiness to detect whether computer or network resources have been compromised. • Perceived ability and readiness to detect whether computer or network resources are being used in support of illegal activities.
Readiness to Prevent Attacks	Perceived Readiness to Prevent Attacks	PR.1.3 PR.1.4 PR.2.2 PR.2.3	• Perceived ability and readiness to prevent a cyberattack from stealing sensitive information.

			• Perceived ability and readiness to prevent a ransom ware attack. • Perceived ability and readiness to prevent a ransom ware from encrypting sensitive data resources.
Readiness to Recover from Attacks	Perceived Readiness to Recover from Attacks	PR.1.5 PR.2.4 PR.2.5	• Perceived ability and readiness to recover users' access to computer resources in the event of a ransom ware attack without paying the ransom. • Perceived readiness to recover data resources after they have been deleted or encrypted as the result of a cyber or ransom ware attack.

4.2 Instrument Validity

Knowledge about a given phenomenon can only be clearly established when it can be successfully demonstrated that the means of measurement accurately represent the theoretical constructs that they are intended to measure. The question then becomes, how can researchers ensure "goodness of fit" between measurement instruments and the theoretical constructs they are intended to measure? The process by which this occurs is known as instrument validation, which has been well articulated in previous research (Cook & Campbell, 1979). Instrument validation seeks to establish several different types of validities. Those validities, along with the questions they seek to answer, are presented in Figure 7. The figure is adopted from Detmar Straub's (1989) article entitled, "Validating Research Instruments".

As Cook and Campbell note, and as Straub's figure indicates, the process of instrument validation should precede other core statistical and empirical validities such as statistical conclusion validity. This is because most statistical tests to establish internal validity and statistical conclusion validity are based on the assumption that the error terms between the

observations are uncorrelated (Hair, et al., 1979; Lindman, 1974). As Straub (1989) notes, if participants in a research study answer in some way that is a function of the instrument instead of the underlying constructs, this assumption will be violated. For statistical tests that are not robust in this regard, a violation of this assumption will present itself in the form of unstable parameter estimates and unusually large standard errors (Lindman, 1974).

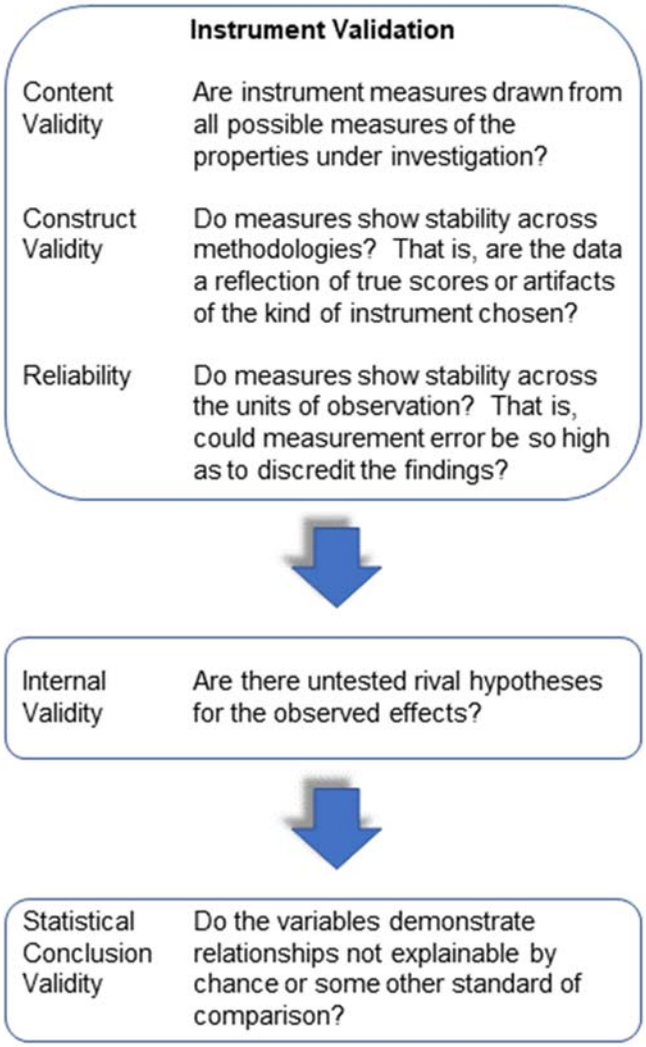

Figure 7: Step by Step Process of Instrument Validity (Straub, 1989)

Construct validity seeks to answer the question of whether the data is measuring a true phenomenon, or is merely an artifact of the measurment instrument itself (Cronbach, 1971;

Campbell & Fiske, 1959). In order to answer this question, correlations between observations are studied. If the observations reflect valid constructs in this sense, then one should expect to see high correlations among measurements that are intended to measure the same construct, even when using different methods, and low correlations between measures that are intended to measure different constructs (Campbell & Fiske, 1959). Campbell and Fiske argue that the multitrait-multimethod (MTMM) approach works well as a means of establishing construct validity. Other methods that have been shown to establish construct validity are confirmatory factor analysis (CFA) and principal components analysis (PCA) (Long, 1983; Nunnally, 1967). Construct validity is established when correlations among similar items, or "traits", are sufficiently associated with one another, but significantly different than zero. This is the case when demonstrating convergent validity. Disimilar items that are sufficiently different from one another demonstrate discriminant validity.

In addition to construct validity, instrument validation is concerned with a measurement instrument's reliability. It is possible that participants' answers on any particular survey item are a function of their understanding of the item instead of the underlying construct it is meant to represent. This can be due either to the way in which the survey was administered, or because the item itself is ambiguous or otherwise misleading. When the responses on one or more survey items differ from alternative measures of those same items, that measurement instrument is said to have poor reliability. Reliability, therefore, is an evaluation of measurement accuracy (Cronbach, 1951). Large Cronbach's alphas indicate high correlations among similar or same items, which is a good indication that the measures are reliable.

Moving beyond instrument validation, internal validity is concerned with whether or not observed effects could be the result of unmeasured variables. In essence, measures of internal

validity seek to determine whether rival explanations, other than the researcher's hypotheses, could be responsible for an instrument's findings. Within the MIS discipline, the importance of establishing internal validity has been previously argued by Jarvenpaa, Dickson, & DeSanctis (1984).

Lastly, statistical conclusion validity is an assessment of whether the mathematical correlations between variables are likely due to chance, or to some true underlying covariation, which is presumed to be the result of the researcher's theoretical assumptions (Cook & Campbell, 1979). Errors in the conclusions regarding true covariation between variables represent violations of statistical conclusion validity, and can be affected by both sample size and the reliability of the measurment instrument. Statistical conclusion validity can also be determined by the power of a statistical test. The statistical power of a test is closely associated with sample size, so that tests which employ larger sample sizes inherently have more power, and are therefore less likely to improperly reject the null hypothesis (Baroudi & Orlikowski, 1989; Cohen, 1969; Kraemer & Thiemann, 1987).

Straub (1989) makes the point that many common statistical techniques, such as regression, MANCOVA, factor analysis, and LISREL, make no conclusions regarding the viability of rival assumptions or the meaningfulness of the underlying theoretical constructs. Statistical conclusions of validity simply evaluate measurement results based on their mathematical correlations. Without prior instrument validation, the possibility remains that those correlations are due to some spurious explanation, such as unaccounted-for moderator variables (Sharma, Durand, & Gur-Arie, 1981), or misspecification of the underlying theoretical model (Blalock, 1969). As Straub notes, conducting instrument validation prior to tests of

statistical conclusion validity strengthens the research study's findings because the effects of extraneous moderator variables and rival hypotheses have been previously controlled for.

Instrument validation will occur on the PACRM measurement instrument in the following manner. Building on Straub's (1989) example for instrument validation, the validation of the PACRM survey will be conducted in three stages. Stages one and two comprise the pilot test phase while stage 3 comprises the roll-out phase. The pilot test phase will test the content validity of the proposed survey while the roll-out phase will test its construct validity and reliability. Lastly, the model will be tested in a structural analysis framework using averaged scores on the measurement variables to represent the constructs.

The instrument is designed to elicit responses from IT managers who are employed at the organizational-unit level at complex, multi-tiered organizations. For the initial study, the organizations targeted will be colleges and universities in the United States. The four groups of factors discussed in Chapter 3 above have been organized into respective blocks of questions on the survey. Each block contains survey questions that correspond to the measurement model elements listed in Table 5.

4.3 Pilot Test Phase Overview

During this phase, the draft survey was presented to IT managers who matched the participant specifications for the project. First, in-depth interviews were conducted with a number of workgroup IT managers working at a large public university in the southeastern United States. Interviewees were prompted to answer open-ended, qualitative questions regarding their cybersecurity practices, their perceptions of the need for awareness to several factors related to computer and network security, and the roles that previous experience in cybersecurity and attitudes towards risk have in shaping their perceptions of their cybersecurity

readiness. The interview questions that were used appear as Appendix A in this document. Concepts that were independently raised by multiple participants were noted and the precise language was recorded in order to capture any perceptual communalities in mental constructs between the participants. This helped to establish the content validity of the instrument.

The second part of stage 1 involved the participants taking an initial draft of the survey, during which they were encouraged to "think aloud." The think-aloud protocol has been previously used in Management Information Systems (MIS) studies where new survey instruments were proposed (Hilkert, et al., 2011), as well as in many psychology studies. Notes were recorded by the primary researcher and any commonalities between respondants were incorporated into subsequent drafts of the survey.

In stage two of the pilot test phase, the survey was administered as a web-based, Qualtrics survey to a number of IT managers working at the school or department level at several colleges and universities throughout the southeastern United States. The survey responses generated during this stage of testing were subjected to tests of reliability using the Cronbach's alpha technique. It has been shown that the reliability and overall construct validity of a proposed instrument can be further established through factorial methods such as Principal Components Analysis (PCA) (Long, 1983; Nunnally, 1967). However, the number of responses were not of a sufficient quantity during stage 2 to conduct a valid PCA analysis. The results of the Cronbach's alpha test, therefore, are shown in Table 12 below.

4.4 Stage 1 Results

Stage 1 consisted of qualitative interviews with a number of IT managers who all work at the decentralized school or department level of a large, public university located in the southeastern United States. During this stage, each manager provided answers to all of the

interview questions and participated in an initial draft of the PACRM survey. Table 6 provides some basic demographic information for this initial test group.

Table 6: Basic Demographic Data for Stage 1 Test Group

Gender	Number of Participants	Approximate Mean Age	Approximate Mean Years of Experience in the IT Field	Approximate Mean Years of Experience in IT Positions in Higher Education	Academic Departments Supported
Male	3	54.17	22.5	17.5	3
Female	1	---	7.5	7.5	1

As can be seen in Appendix A of this document, the interview questions were designed to elicit responses to the factors that were thought to be relevant to increasing an IT manager's level of cybersecurity readiness. Respondents were asked to assess the roles that best practices, awareness of computer and network security, previous level of experience in cybersecurity, the number and type of cybersecurity-related certifications, and the importance of attitudes towards risk had in shaping their perceptions of their cybersecurity readiness. The frequency of common responses, which reflect the managers' answers for each survey question are listed below in Tables 7-11.

Table 7: Stage 1 Frequency of Answers Related to Specific Elements for Question 1 - Best Practices

Educate User Community	Operating System and Application Management	Use of Preventative Software Measures	Control Physical Access	Use of Backup Procedures	Use of Encryption
3	2	2	2	1	1

Table 8: Stage 1 Frequency of Answers Related to Specific Elements for Question 2 - Awareness of Network Security

Know Your Contacts in	Keep up to Date on	Understand It to the Level	Be a Good Educator

the Organization	Current Threats	of Your Responsibility	
2	1	1	1

Table 9: Stage 1 Frequency of Answers Related to Specific Elements for Question 3 - Importance of Previous Experience with Cybersecurity

Training is an Important but not Key Factor	Previous Experience with Being Hacked is Vital	Self-Education / Continuing Education is the Key
1	1	3

Table 10: Stage 1 Frequency of Answers Related to Specific Elements for Question 4 - Importance of the Number and Type of Certifications

Certifications Are an Important Factor	Certifications Are Not Important	Depends on the Type of Certification
1	2	1

Table 11: Stage 1 Frequency of Answers Related to Specific Elements for Question 5 - Importance of Attitudes Towards Risk

Important to be Risk Avoidant	Awareness of Risk is Important
3	1

The relatively high frequency of responses that were generated in the pre and post-survey interview questions that stressed the importance of educating the user community on issues related to information security led to the inclusion of the *Degree of User Community Awareness of Security Issues* factor in the PACRM model and an additional block of survey questions on the instrument. These changes are reflected in Appendix A as well as in the PACRM model, illustrated in Figures 1 and 6 of this dissertation. Overall, the pre-test stage 1 qualitative interview questions were helpful in refining the content validity of the survey questions. For example, in addition to the inclusion of the additional factor, the negative reaction that was

evident in the responses, with regard to the number and type of cybersecurity-related certifications, combined with the ubiquity with which the managers indicated that they had zero cybersecurity-related certifications, led to the thinking that this factor should be removed from the model. Although it was evident that it should not be part of the present analysis, the question was left in the survey to gather data for future research. Therefore, the survey was modified to combine multiple questions related to that subject into a single, optional question that asks respondants to list any cybersecurity-related certifications that they currently hold.

Likewise, the "think aloud" protocol that the managers engaged in while taking the initial draft of the survey instrument highlighted many potential areas for improvement. Primarily, each of the managers surveyed found the survey length to be "reasonable," "okay," and "about right." One of the respondants remarked that age should be the first question in the survey, and this was deemed a reasonable suggestion. As such, that change was made in subsequent drafts of instrument. In addition, two areas of concern with the survey became evident through this exercise. First, several of the managers visibly reacted to the question about their level of experience with initiating cyberattacks. Recall that this reaction was anticipated during the conceptual development phase of the project, which is why the item was designed as one component of a summative measure. Furthermore, the data shows a tendency towards a possible floor effect on this item with the majority of managers (n=3) indicating "No Experience at All" and the last manager (n=1) indicating "a Little Experience." While no conclusions can be made from such a small sample size, the visceral reaction that the majority of managers displayed indicates that the researchers were correct in anticipating a floor effect for this measure.

Second, the think aloud exercise also demonstrated a degree of confusion among the managers with respect to the perceived awareness questions. These questions are included as

PA.2 in Appendix B. All four managers expressed audible consternation at the wording in that particular grouping. In post-survey followup questions, it was determined that every manager who supported a user community felt uncomfortable with their level of security. However, they felt powerless to do anything about it because so much of the responsibility for securing work computers lies with the user community. This was deemed to be further evidence of the need for an additional block of questions related to user community awareness of security issues. Furthermore, this block of questions was placed ahead of the perceived awareness questions in the survey as a way to ameliorate managers' overall level of concern.

4.5 Stage 2 Results

Stage 2 consisted of 25 total responses from workgroup IT managers working at colleges and universities throughout the southeastern United States. Frequency distributions for participant age and years of experience in IT by gender are shown in Figures 8 and 9 below.

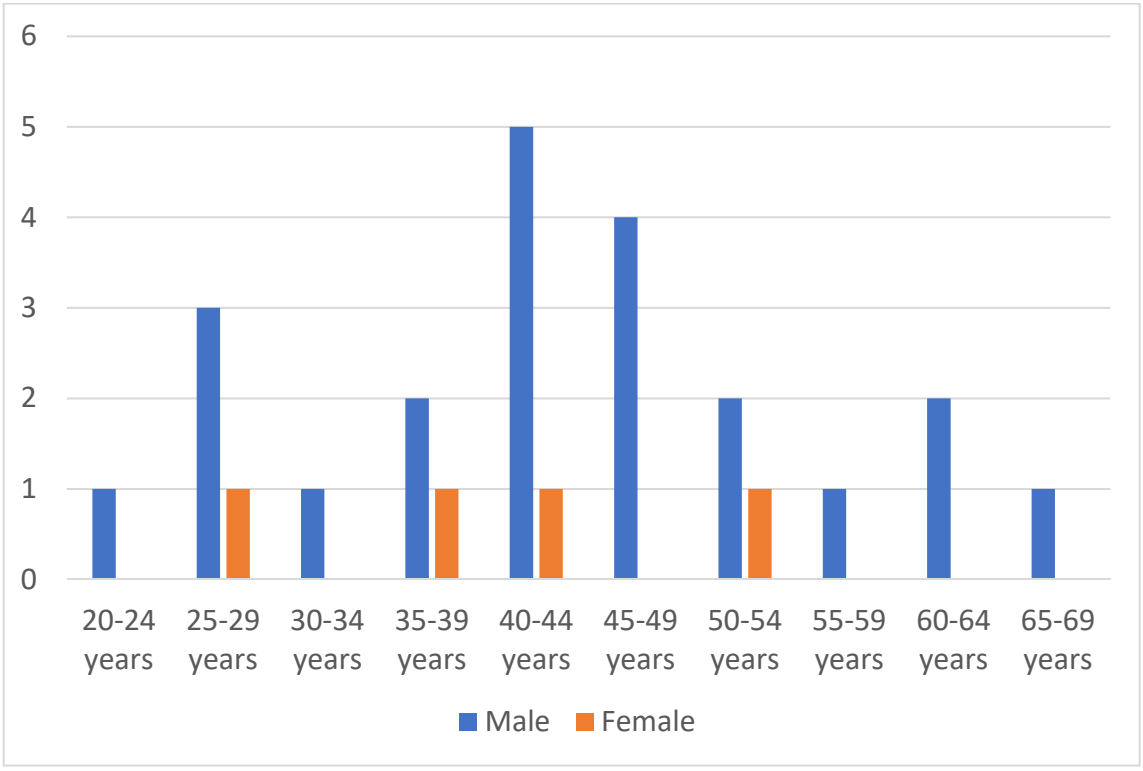

Figure 8: Frequency of Stage 2 Participants by Age in Years Broken Out by Gender

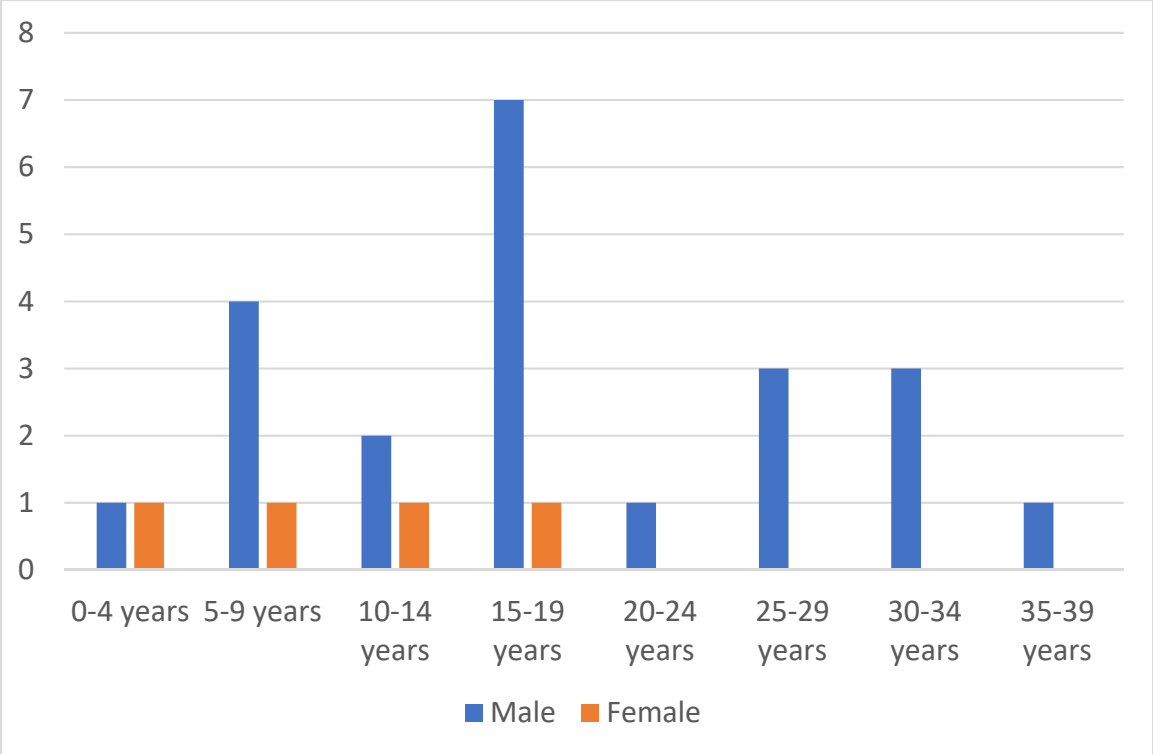

Figure 9: Frequency of Stage 2 Participants by Years of Experience in IT Broken Out by Gender

The measure asking about participants' experience with initiating cyberattacks continued to be low at this stage of data collection, as evidenced by a mean value of 1.48. This indicates that the majority of managers surveyed stated that they had a little experience or no experience at all with initiating cyberattacks. Because the question contained language that made it clear that legitimate hacking, such as might be performed as part of a training program or as a Certified Ethical Hacker (CEH), was to be included, the results indicate either a reluctance on the part of IT managers to divulge what may be illicit activities or genuine inexperience. If this trend is also seen in stage 3 of this study, it may indicate a possible area of intervention for cybersecurity-related training. By holding hacking training where IT managers participate in simulated hacking exercises, it may be possible to raise manager's perceptions of their own cybersecurity readiness.

Cronbach's alpha statistics were generated for the 25 cases for all of the constructs listed in Table 5 of this dissertation. The overall statistics, which are presented in Table 12 below, show that a majority of the factors show good reliability. Of the thirteen constructs tested, 10 had Cronbach's alpha values of .70 or above. The value of .70 is, of course, a guideline for demonstrating good reliability among measures. However, previous MIS researchers have, on occasion, adopted lower values. For example, Siponen et al., adopted a threshold value of .608 to demonstrate internal reliability of their measures (2010). In this study, *Perceived Awareness of Immediate Threat Environment* had a Cronbach's alpha of .663, which indicates that a change of wording may be appropriate in future drafts of the survey for some of the questions that are associated with this measure.

Table 12: Cronbach's Alpha Statistics for Stage 2 PACRM Constructs

Construct	Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	Number of Items
Level of Previous Experience with Cybersecurity	.722	.741	3
Personal Risk Avoidance Score	.476	.475	3
Extent of Use of Network Activity Monitoring Mechanisms	.939	.939	6
Extent of Control over Physical Access to Network Resources	.805	.814	4
Extent of Use of Preventative Software Measures	.915	.912	12
Extent of Use of a Backup Policy Where Backups are Kept Offline	.876	.879	2
Degree of User Community Awareness of Security Issues	.861	.865	6

Perceived Awareness of Immediate Threat Environment	.663	.639	4
Perceived Awareness of Vulnerabilities in Physical Infrastructure	.795	.788	5
Perceived Awareness of Defensive Measures in Place	.012	.012	2
Perceived Readiness to Detect Attacks	.813	.811	3
Perceived Readiness to Prevent Attacks	.920	.921	4
Perceived Readiness to Recover from Attacks	.916	.919	3

The risk measure demonstrated exceedingly poor reliability with a Cronbach's alpha of .476, which indicates that a significant rewording of the questions associated with this measure is needed. In addition, Cronbach's alpha statistics will need to be generated on the stage 3 data set to ensure that all the proposed constructs demonstrate good reliability before proceeding with further analysis.

Lastly, *Perceived Awareness of Defensive Measures in Place* had a Cronbach's alpha of .012. There were just two items associated with this measure and on closer inspection, it was deemed that they were, in fact, measuring two very different things. Specifically, the two items attempted to capture the IT manager's level of knowledge and comfort with the defensive measures that he or she has in place to keep his or her supported computer resources secure. Since the nature of *Perceived Awareness of Defensive Measures in Place* is, in fact, a measure of the IT manager's level of awareness with the defensive measures that he or she has in place, the most prudent course of action is to alter the language of the measure to make that more explicit. In that case, the construct should then be retested for reliability before proceeding with further analysis.

4.6 Roll-Out Phase Overview

In stage 3 of the project, approximately 160 IT managers who work at the school or department level of colleges and universities in other regions of the United States were surveyed. This final group of participants represented unit-level IT administration in line with the proposed scope of the project. Due to the complexities of modeling the effects of organizational culture on individual behavior, it was not deemed prudent to survey multiple individuals per institution. This is especially true given the relatively small number of responses that were collected. Therefore, one individual per institution was surveyed to ameliorate the confounding effect of observations that are grouped within institutions.

To ensure that this procedure was followed, the principal researcher personally contacted individuals at colleges and universities via email or phone. This was necessary to describe the nature of the project and to determine whether each potential subject meets the demographic specifications of the target population. The principal researcher then attempted to discern whether each potential respondent was a workgroup IT manager who is working at the school or department level prior to cultivating the actual survey response. In this way, the researcher sought to ensure a high degree of applicability and appropriateness of the underlying data set. Furthermore, the fact that only one response was gathered from each institution hopefully guaranteed a broad generalizability of the data.

4.7 Psychometric Analysis Overview

Additional Cronbach's alpha statistics were run on the full stage 3 data set to test whether the revised survey displayed good reliability for the complete set of measures. A Confirmatory Factor Analysis (CFA) was then performed to examine the underlying characteristics of the measurement model as well as the convergent and discriminant validity of the constructs.

4.8 Structural Model Analysis Overview

Since this is an exploratory study with a limited number of observations, the researcher used average scores to represent each of the constructs. Given the complexity of the conceptual model, stage 3 simply did not garner enough observations to allow for a full Structural Equation Model (SEM) of the underlying PACRM theoretical and measurement models at the same time. However, the previous round of psychometric analysis helped to validate the underlying measurement model, so that a full SEM analysis proved redundant at this stage. Rather, a path analysis was conducted to validate the proposed paths.

4.9 Stage 3 Results

Stage 3 of the PACRM instrument validation process was conducted over a twenty-two-week period from mid-January to mid-June of 2018. During that time, 1,030 individual IT administrators who work at 4-year public colleges and universities across the United States were contacted through a combination of electronic mail and telephone. The panel resulted in 161 survey responses, which represents a final conversion rate of 15.631 percent. Of the 161 survey responses submitted, 26 of them were removed due to partial or incomplete responses. These responses were deleted using listwise deletion. Therefore, the final stage 3 dataset consisted of 135 complete responses with no missing data.

The survey was fully anonymized within the Qualtrics research system so that the researcher was unable to match responses to individual panel members beyond the institutional level. This was done intentionally to maintain the maximum practical anonymization of the data at this stage of the collection process. To ensure maximum variability between institutions, only three respondents were contacted per institution. Once the researcher could feasibly rule out the potential for duplicate responses arising from the same institution, the distributions were deleted

after thirty days, thereby eliminating the researcher's ability to match responses at the institutional level. Institutions were identified through a database query from the National Center for Education Statistics on December 12, 2017 in which the names and web site addresses of all 4-year, public higher education institutions in the United States were pulled (National Center for Education Statistics).

As was the case with the Stage 2 results, frequency distributions for participant age and years of experience in IT by gender are shown in Figures 10 and 11 below.

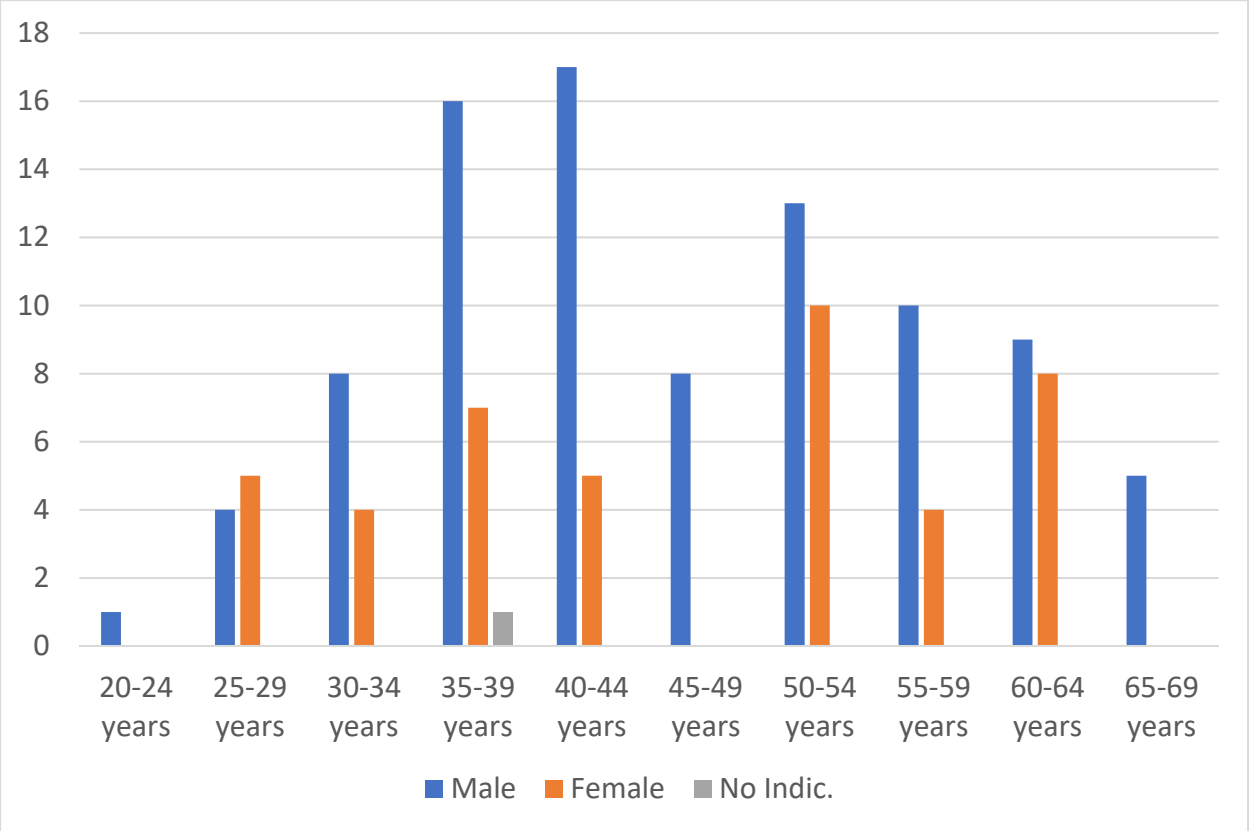

Figure 10: Frequency of Stage 3 Participants by Age in Years Broken Out by Gender

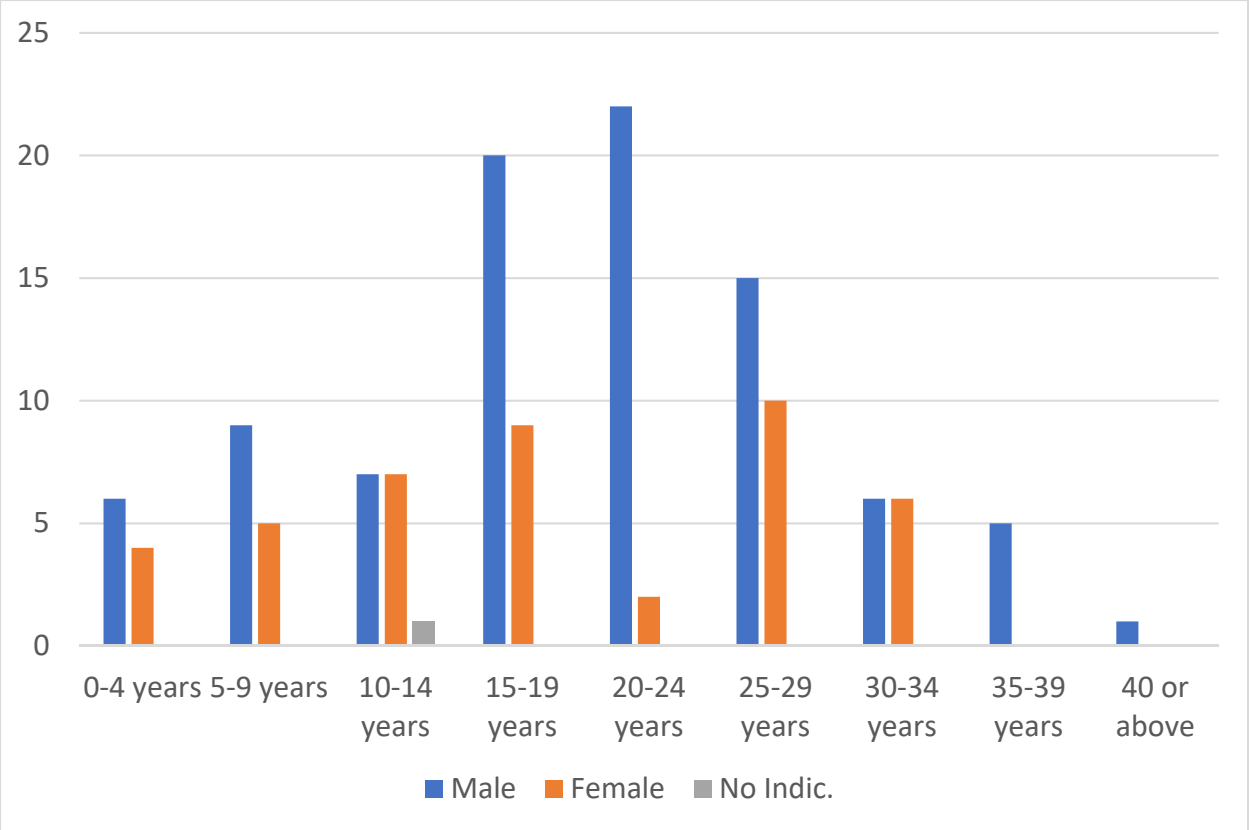

Figure 11: Frequency of Stage 3 Participants by Years of Experience in IT Broken Out by Gender

4.10 Pretest Study Results

To establish construct validity on the PACRM survey, a CFA was run on the stage 3 dataset using the SPSS AMOS statistical package, version 25. Prior to running the CFA, the factorability of the dataset was tested using the Kaiser-Meyer-Olkin measure of sampling adequacy (KMO MSA) technique. The KMO MSA statistic showed that the dataset displayed good overall factorability with a value of .874.

The CFA essentially tests the measurement model listed in Table 5 of this dissertation. It tests the pattern of relationships between the measurement model and the latent constructs hypothesized. Prior to running the CFA, however, Cronbach's alpha statistics were once again generated for the 135 cases in the stage 3 dataset. The overall statistics, which are presented in

Table 13 below, show that all the factors displayed good reliability, as denoted by a Cronbach's alpha of .70 or above.

Table 13: Cronbach's Alpha Statistics for Stage 3 PACRM Constructs

Construct	Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	Number of Items
Level of Previous Experience with Cybersecurity	.700	.741	3
Personal Risk Avoidance Score	.766	.765	3
Extent of Use of Network Activity Monitoring Mechanisms	.929	.929	6
Extent of Control over Physical Access to Network Resources	.775	.776	4
Extent of Use of Preventative Software Measures	.905	.906	12
Extent of Use of a Backup Policy Where Backups are Kept Offline	.826	.832	2
Degree of User Community Awareness of Security Issues	.883	.884	6
Perceived Awareness of Immediate Threat Environment	.904	.904	4
Perceived Awareness of Vulnerabilities in Physical Infrastructure	.882	.886	4
Perceived Awareness of Defensive Measures in Place	.814	.820	2
Perceived Readiness to Detect Attacks	.889	.891	3
Perceived Readiness to Prevent Attacks	.908	.908	4
Perceived Readiness to Recover from Attacks	.888	.891	3

As stated above, the CFA is based on the survey responses from 135 workgroup IT managers who work at institutions of higher learning across the United States. Since the number of observations in the dataset was lower than what would be needed for a full-scale analysis, the full measurement model was subdivided into three subset models of theoretically related factors (Bentler & Chou, 1987). These factor groups were the four practice related factors enumerated above together with the previous experience and risk factors, the three awareness factors, and the user community awareness factor. In each sub-model, the group of factors were tested in relation to the three response factors, which represent the IT manager's perceived readiness to detect, prevent, and recover from a cyberattack.

Kline (2005) suggests that appropriate model fit indices to include from a CFA are the Chi-Square test, the Comparative Fit Index (CFI), the Root Mean Square Error of Approximation (RMSEA), and the Standardized Root Mean Square Residual (SRMR). The Chi-Square (χ^2) statistic has been the traditional parameter for making judgements about the acceptability of model fit (Hu & Bentler, 1999). A good fitting model would result in an insignificant result at the .05 threshold. There are, however, a number of severe restrictions on its use. Primarily, departures from multivariate normality in the data may result in model rejections even in models that are properly specified (Hooper et al., 2008). Secondly, Chi-Square is sensitive to sample size. Therefore, the Chi-Square statistic nearly always rejects the model where datasets are large enough (Bentler & Bonett, 1980). For these reasons, alternative fit statistics have been sought out. One such statistic is the Chi-Square to degrees of freedom ratio (Wheaton et al., 1977). Generally speaking, a chi-square/d.f. ratio of less than 3.0 indicates an acceptable level of fit (Marsh et al., 2004), although values as high as 5.0 (Wheaton et al., 1977) and as low as 2.0 (Tabachnick & Fidell, 2007) have also been argued for.

The Comparative Fit Index (Bentler P. , 1990) is a revised form of the Normed Fit Index (NFI) that takes into account sample size. Compared with the NFI, the CFI performs well even when sample size is small (Tabachnick & Fidell, 2007). As with the NFI, CFI values range from zero to 1.0 with values closer to 1.0 indicating good model fit. A cut-off point greater than .90 has been generally been accepted as the standard needed to ensure that misspecified models are not accepted (Hu & Bentler, 1999). Finally, the Standardized Root Mean Square Residual (SRMR) index indicates the difference between the square root of the residuals of the sample covariance matrix and the hypothesized covariance model (Kline, 2005). As with the Root Mean Square Error Approximation (RMSEA), values below .06 indicate a good model fit. However, it has been argued that values as high as .08 are acceptable for both statistics (Hu & Bentler, 1999).

4.11 Subset Model 1: Practice Related Factors

Four Extent of Use constructs were originally hypothesized. These included *Extent of Use of Network Activity Monitoring Mechanisms*, *Extent of Control over Physical Access to Network Resources*, *Extent of Use of Preventative Software Measures*, and *Extent of Use of a Backup Policy Where Backups are Kept Offline*. These four factors were placed into a CFA model together with the *Level of Previous Experience with Cybersecurity* and *Personal Risk Avoidance* constructs, since these six constructs were hypothesized to have relationships with the dependent factors, as illustrated in Figures 1 and 6 of this dissertation. Upon examing the factor loadings, it was determined that five measurement variables could be dropped from further analysis since these variables had loadings on their respective factors that were less than the traditional .5 threshold. Furthermore, it was clear from the initial loadings that the *Extent of Use of Preventative Software Measures* was, in fact, a combination of two latent factors. Three of the measurement variables (the ones related to software preventative measures) loaded together as a

group while the remaining six variables (the ones related to frequency of use of preventative measures) loaded as a noticably distinct second group on the factor. Therefore, a new CFA was performed, which reflected these loadings. The Chi-Square to degrees of freedom ratio was 2.573 (χ^2=1325.042, d.f.=515), with a CFI of .809, and an SRMR of .0754. Table 14 lists the CFA measurement variables and their related constructs along with the variables that were dropped after the initial analysis due to low factor loadings.

Table 14: Practice Related Factors and their Associated Measurement Variables

Construct	Drop	Item Number	Standardized Regression Weight
Level of Previous Experience with Cybersecurity	~~drop~~	~~PE.3~~	~~.412~~
		PE4.1	.873
		PE4.2	.667
Personal Risk Avoidance Score		D8.1	.594
		D8.2	.813
		D8.3	.679
Extent of Use of Network Activity Monitoring Mechanisms		EU1.1	.744
		EU1.2	.785
		EU1.3	.736
		EU2.1	.905
		EU2.2	.944
		EU2.3	.854
Extent of Control over Physical Access to Network Resources		EU1.4	.893
		EU1.5	.861
	~~drop~~	~~EU1.6~~	~~.362~~
		EU2.4	.722
Extent of Use of Preventative Software Measures	~~drop~~	~~EU1.7~~	~~.435~~
	~~drop~~	~~EU1.8~~	~~.449~~
	~~drop~~	~~EU1.9~~	~~.464~~
		EU1.10	.931

		EU1.11	.764
		EU1.12	.762
Frequency of Use of Preventative Measures		EU2.5	.514
		EU2.6	.920
		EU2.7	.927
		EU2.8	.871
		EU2.9	.805
		EU2.10	.750
Extent of Use of a Backup Policy Where Backups are Kept Offline		EU1.13	.729
		EU2.11	.985
Perceived Readiness to Detect Attacks		PR1.1	.824
		PR1.2	.909
		PR2.1	.833
Perceived Readiness to Prevent Attacks		PR1.3	.946
		PR1.4	.885
		PR2.2	.800
		PR2.3	.813
Perceived Readiness to Recover from Attacks		PR1.5	.832
		PR2.4	.869
		PR2.5	.881

4.12 Subset Model 2: Awareness Related Factors

The second CFA tested the construct validity of the awareness group of factors from the original PACRM measurement model. The factors that were included in this group included *Perceived Awareness of the Immediate Threat Environment*, *Perceived Awareness of Vulnerabilities in the Physical Infrastructure*, and *Perceived Awareness of the Defensive Measures in Place*. As was the case with subset model 1, these three factors were put into a

CFA with the three perceived readiness constructs. The resulting CFA had a Chi-Square to d.f. ratio of 4.587 (χ^2=711.009, d.f.=155), CFI of .807, and SRMR of .0649. No measurement variables were dropped after the initial CFA on subset model 2 because there were none that had standardized loadings of less than .5 on their respective factors. Table 15 lists the CFA measurement variables and their related constructs.

Table 15: Awareness Related Factors and their Associated Measurement Variables

Construct	Drop	Item Number	Standardized Regression Weight
Perceived Awareness of Immediate Threat Environment		PA1.1	.853
		PA1.2	.831
		PA2.1	.872
		PA2.2	.799
Perceived Awareness of Vulnerabilities in the Physical Infrastructure		PA1.3	.751
		PA1.4	.820
		PA2.3	.840
		PA2.4	.846
Perceived Awareness of Defensive Measures in Place		PA1.5	.829
		PA2.5	.836
Perceived Readiness to Detect Attacks		PR1.1	.797
		PR1.2	.882
		PR2.1	.872
Perceived Readiness to Prevent Attacks		PR1.3	.901
		PR1.4	.856
		PR2.2	.799
		PR2.3	.818
Perceived Readiness to		PR1.5	.802

Recover from Attacks		PR2.4	.894
		PR2.5	.891

4.13 Subset Model 3: User Community Awareness Factor

The final subset model that was tested was *Degree of User Community Awareness of Security Issues*. As was the case with the previous sub-models, the three perceived readiness factors were included in the analysis. The resulting CFA had a Chi-Square to d.f. ratio of 3.405 (χ^2=333.653, d.f.=98), a CFI of .867, and an SRMR of .0761. No measurement variables were dropped after the initial CFA on subset model 3 because there were none that had standardized loadings of less than .5 on their respective factors. Table 16 lists the CFA measurement variables and their related constructs.

Table 16: User Community Awareness of Security Issues Factor and Associated Measurement Variables

Construct	Drop	Item Number	Standardized Regression Weight
Degree of User Community Awareness of Security Issues		ED1.1	.774
		ED1.2	.687
		ED1.3	.835
		ED1.4	.844
		ED1.5	.609
		ED1.6	.745
Perceived Readiness to Detect Attacks		PR1.1	.808
		PR1.2	.876
		PR2.1	.871
Perceived Readiness to Prevent Attacks		PR1.3	.890
		PR1.4	.850
		PR2.2	.815

		PR2.3	.823
Perceived Readiness to Recover from Attacks		PR1.5	.818
		PR2.4	.881
		PR2.5	.888

4.14 Methodology Summary

This chapter provided an overview of the methodology that was undertaken to validate the PACRM survey instrument. Over the course of approximately nine months, three distinct stages of instrument validation stages took place. The first two stages comprised the pilot test phase in which both qualitative interviews and a pilot study were conducted on the proposed PACRM survey. This phase helped to establish the content validity of the survey instrument. In addition, reliability statistics were generated on the initial pilot test data (n=25) gathered from IT administrators working at 4-year public colleges and universities in the southeastern United States. These reliability statistics showed that several of the survey items needed to be reworked in subsequent drafts of the PACRM survey.

Stage 3 of the instrument validation process consisted of a larger study of 161 workgroup IT managers at colleges and universities across the United States. The construct validity of the survey items was aided by another round of reliability testing in which all of the PACRM constructs were found to have good reliability, as denoted by Cronbach's alphas of .70 or above. Futhermore, Confirmatory Factor Analyses were conducted using the IBM SPSS Amos software, version 25. The original PACRM measurement model, outlined in Table 5 of this dissertation, was divided into three, theory-related submodels, each specifying a different group of factors from within the larger PACRM measurement model. These analyses resulted in several of the measurement variables being dropped due to low factor loadings. In addition, *Extent of Use of*

Preventative Software Measures was found to actually be a confounding of two, distinct latent variables. It was partitioned out accordingly and each of the associated measurement variables were found to load highly on their respective factors. Admittedly, the fit indices for each of the sub-models are not great, although they are close to the traditional accepted boundaries. This is, in some ways, to be expected as the individual sub-models by no means represent the most parsimonious or complete solutions.

In the next chapter, the three submodels were recombined into a new, more parsimonious full measurement model. A new Confirmatory Factor Analysis was then performed on the full model and the constructs were examined for evidence of convergent and discriminant validity. Finally, the path analysis was conducted in IBM SPSS Amos using the participants' averaged scores from the measurement variables to represent the latent constructs.

5 RESULTS

5.1 Confirmatory Factor Analysis of Full Measurement Model Results

In order to ensure a good parameter estimate to observation ratio (Vorhies & Morgan, 2005), the full PACRM measurement model was divided into three subsets of theoretically related submodels (Bentler & Chou, 1987). Due to the low number of observations relative to the complexity of the overall model, this was done in the model trimming stage so that measurement variables that did not load well on their respective factors could more easily be identified. In this way, five measurement variables were dropped from further analysis due to loadings that were below the .5 threshold on their respective factors. In addition, *Extent of Use of Preventative Software Measures* was divided into two distinct latent factors. The first, *Extent of Use of Preventative Software Measures*, contains three measurement variables while the second, *Frequency of Use of Preventative Measures*, contains six measurement variables.

As the next step in the CFA process, the three submodels were recombined into a full measurement model and a new CFA was performed using the stage 3 dataset of 135 observations. The CFA had a Chi-Square to d.f. ratio of 2.274 (χ^2=2575.918, d.f.=1133), a Comparative Fit Index of .778, an RMSEA value of .097, and a Standardized Root Mean Square Residual value of .0782. None of these values represent a good model fit although the Chi-Square to d.f. ratio and SRMR values are within traditional boundaries for acceptable model fit for those statistics (Marsh et al., 2004; Hu & Bentler, 1999).

5.2 Convergent/Discriminant Validity of Full Measurement Model Results

Convergent validity is the agreement between measures of the same construct while discriminant validity is the distinctiveness between different constructs (Campbell & Fiske, 1959). Table 17 lists the validity and reliability statistics for all of the constructs in the full measurement model.

Table 17: Validity and Reliability Statistics for the Full Measurement Model Constructs

	CR	AVE	MSV	MaxR(H)
UsrCommA	0.886	0.568	0.183	0.899
PrevExpe	0.750	0.604	0.291	0.801
NwActMon	0.931	0.694	0.432	0.950
PhysCtrl	0.867	0.687	0.473	0.885
PrvSWMea	0.861	0.676	0.265	0.902
FrPrvMea	0.918	0.658	0.567	0.947
RgOffBck	0.854	0.749	0.567	0.964
PRDetect	0.888	0.727	0.880	0.895
PRPrevnt	0.908	0.712	0.880	0.917
PRRecovr	0.898	0.746	0.740	0.905
RskAvoid	0.741	0.492	0.250	0.772
AwarThrt	0.906	0.707	0.876	0.911
AwarVuln	0.888	0.664	0.996	0.891
AwarDefM	0.819	0.694	0.996	0.820

As seen by the Composite Reliability (CR) column, all of the constructs show good overall reliability. The Average Variance Extracted (AVE), which measures the average amount of variance in the measurement variables explained by their respective constructs, is an indication of convergent validity. As can be seen in Table 17, the AVE for each of the factors except *Personal Risk Avoidance* are above the .5 treshold. This indicates that the constructs in the PACRM measurement model were generally successful in accounting for more than half of the observed variance in the measurement variables. The low AVE value for the *Personal Risk Avoidance* factor is the one exception to this pattern. However, given the fact that this construct

shows both good reliability and discriminant validity, it is not overally problematic for the analysis.

Of greater concern is the fact that *Perceived Readiness to Detect an Attack* and *Perceived Readiness to Prevent an Attack* show a degree of discriminant validity violations with one another. This can be seen in Table 17 by the fact that the AVE is less than the Maximum Shared Variance (MSV) for each of these factors. This indicates that there is some correlation between the two constructs. This also seems to be the case with the three awareness-related factors. All three constructs, *Perceived Awareness of the Immediate Threat Environment, Perceived Awareness of Vulnerabilities in the Physical Infrastructure,* and *Perceived Awareness of Defensive Measures* seem to be highly correlated with one another. These correlations are readily apparent in the Factor Correlation Matrix, shown in Table 18 below.

Table 18: Factor Correlation Table

	UsrComA	**PrevExpe**	**NwActMon**	**PhysCtrl**	**PrvSWMea**	**FrPrvMea**	**RgOffBck**	**PRDetect**	**PRPrevnt**	**PRRecovr**	**RskAvoid**	**AwarThrt**	**AwarVuln**	**AwarDefM**
UsrComA	**0.754**													
PrevExpe	0.066	**0.777**												
NwActMon	0.096	0.536	**0.833**											
PhysCtrl	0.189	0.442	0.569	**0.829**										
PrvSWMea	0.177	0.166	0.249	0.451	**0.822**									
FrPrvMea	0.160	0.415	0.657	0.688	0.515	**0.811**								
RgOffBck	0.073	0.405	0.618	0.687	0.438	0.753	**0.866**							
PRDetect	0.366	0.420	0.623	0.661	0.499	0.566	0.491	**0.852**						
PRPrevnt	0.428	0.472	0.582	0.598	0.418	0.542	0.452	0.938	**0.844**					
PRRecovr	0.353	0.483	0.512	0.646	0.437	0.516	0.500	0.843	0.860	**0.864**				
RskAvoid	0.068	-0.500	-0.231	-0.096	0.024	-0.271	-0.161	-0.181	-0.095	-0.124	**0.701**			
AwarThrt	0.352	0.539	0.598	0.606	0.296	0.481	0.479	0.708	0.708	0.584	-0.092	**0.841**		
AwarVuln	0.394	0.498	0.600	0.667	0.378	0.546	0.501	0.840	0.782	0.739	-0.063	0.936	**0.815**	
AwarDefM	0.305	0.438	0.606	0.608	0.407	0.568	0.541	0.868	0.769	0.718	-0.032	0.901	0.998	**0.833**

In order to determine the source of the factor correlation, the factor score weights for each of the constructs were examined. Upon closer inspection, it was found that there was significant cross-loading between *Perceived Awareness of Vulnerabilities in the Physical Infrastructure* and *Perceived Awareness of Defensive Measures*, such that all of their measurement variables loaded highly on both constructs.

Table 19: Factor Loadings for Three Perceived Awareness Constructs

Item Number	Expected Factor	Actual Factor	Perceived Awareness of Defensive Measures	Perceived Awareness of Vulnerabilities in the Physical Infrastructure	Perceived Awareness of the Immediate Threat Environment
PA1.1	AwarThrt	AwarThrt	.066	.075	.202
PA1.2	AwarThrt	AwarThrt	.059	.067	.182
PA1.3	AwarVuln	AwarVuln	.053	.079	.044
PA1.4	AwarVuln	AwarVuln	.072	.108	.060
PA1.5	AwarDefM	AwarDefM	.106	.077	.051
PA2.1	AwarThrt	AwarThrt	.055	.063	.169
PA2.2	AwarThrt	AwarThrt	.037	.042	.113
PA2.3	AwarVuln	AwarVuln	.091	.136	.075
PA2.4	AwarVuln	AwarVuln	.091	.136	.075
PA2.5	AwarDefM	AwarDefM	.134	.099	.065

This result was not theorized and so it is difficult to discern exactly what second-order factor is causing the cross-loadings between these two factors. An educated guess can be made that the four measurement variables, which attempted to assess the IT manager's knowledge and awareness of his or her organizational unit's network physical design and vulnerability to attack, were actually read by participants as indicators of their preparedness for a cyberattack. Similarly, the two survey items that questioned the IT managers on their knowledge and

awareness of any defensive measures that were in place to protect their networks may also have been read by study participants as indicators of their preparedness.

The factor loadings also show that the high correlation between *Perceived Readiness to Detect Attacks* and *Perceived Readiness to Prevent Attacks* were caused by items cross-loading between these two factors, although not to the degree seen in the perceived awareness constructs. Table 20 has the factor loadings for the three perceived readiness constructs, along with their measurement variables.

Table 20: Factor Loadings for Three Perceived Readiness Constructs

Item Number	Expected Factor	Actual Factor	Perceived Readiness to Recover from an Attack	Perceived Readiness to Prevent Attacks	Perceived Readiness to Detect Attacks
PR1.1	PRDetect	PRDetect	.014	.058	.084
PR1.2	PRDetect	PRDetect	.023	.095	.136
PR1.3	PRPrevnt	PRPrevnt	.063	.241	.111
PR1.4	PRPrevnt	PRPrevnt	.038	.147	.067
PR1.5	PRRecovr	PRRecovr	.137	.025	.011
PR2.1	PRDetect	PRDetect	.020	.084	.121
PR2.2	PRPrevnt	PRPrevnt	.028	.106	.048
PR2.3	PRPrevnt	PRPrevnt	.029	.110	.050
PR2.4	PRRecovr	PRRecovr	.277	.051	.021
PR2.5	PRRecovr	PRRecovr	.263	.049	.020

The measurement variables all loaded on their expected factors. However, the items pertaining to the IT manager's perceived ability to detect if his or her computer resources were being used in support of illicit activities and the item related to his or her readiness to detect if a computer resource had been hacked, both loaded highly on *Perceived Readiness to Detect Attacks* and *Perceived Readiness to Prevent Attacks*. It may be that the specificity of these two

questions triggered a prevention response in the minds of the IT administrators, in addition to the detect response that was theorized.

Table 21 lists the complete set of measurement variables that were used in the final measurement model, together with their respective regression weights.

Table 21: Full Measurement Model Constructs with Their Associated Measurement Variables

Construct	Item Number	Item Description	Standardized Regression Weight
Level of Previous Experience with Cybersecurity	PE4.1	Indicate your level of previous experience with each of the following items: Preventing or stopping cyberattacks?	.874
	PE4.2	Indicate your level of previous experience with each of the following items: Initiating cyberattacks? (Either as part of an advanced cybersecurity certification training program, or as a Certified Ethical Hacker, or on your own)	.666
Personal Risk Avoidance Score	D8.1	Indicate your level of agreement to each of the following items: In general, I try to avoid risk whenever possible at work.	.606
	D8.2	Indicate your level of agreement to each of the following items: I am not comfortable accepting risk in matters related to my job.	.818
	D8.3	Indicate your level of agreement to each of the following items: I am not comfortable accepting risk when it comes to the information security of my department.	.663
Extent of Use of Network Activity Monitoring Mechanisms	EU1.1	Indicate the extent to which you use each of the following items for the technology in your unit: Network activity logging mechanisms to monitor network activity?	.749
Extent of Use of Network Activity Monitoring	EU1.2	Indicate the extent to which you use each of the following items for the technology in your unit: Intrusion Detection Systems (IDS) and/or	.791

Mechanisms (cont.)		Intrusion Prevention Systems (IPS) on your network?	
	EU1.3	Indicate the extent to which you use each of the following items for the technology in your unit: Sensor deployments and/or traffic analyzers for your network?	.742
	EU2.1	Indicate the frequency for which each of following items is true for the technology in your unit: You monitor general network activity logs for signs of suspicious network activity?	.904
	EU2.2	Indicate the frequency for which each of following items is true for the technology in your unit: You check the probing and/or block reports from any Intrusion Detection Systems (IDS) and/or Intrusion Prevention Systems (IPS) on your network?	.941
	EU2.3	Indicate the frequency for which each of following items is true for the technology in your unit: You analyze reports or data from a sensor deployment (e.g., honeypots, traffic analyzers other than your IDS/IPS, etc.) for your network?	.852
Extent of Control over Physical Access to Network Resources	EU1.4	Indicate the extent to which you use each of the following items for the technology in your unit: Physical controls to prevent unauthorized physical access to network and server resources?	.894
	EU1.5	Indicate the extent to which you use each of the following items for the technology in your unit: Locked rooms and/or server cabinets to secure servers or other vital computer resources?	.853
Extent of Control over Physical Access to Network Resources (cont.)	EU2.4	Indicate the frequency for which each of following items is true for the technology in your unit: You control unauthorized access to server and network resources?	.731

Extent of Use of Preventative Software Measures	EU1.10	Indicate the extent to which you use each of the following items for the technology in your unit: Computers that are protected with antivirus software?	.930
	EU1.11	Indicate the extent to which you use each of the following items for the technology in your unit: Computers that are protected with anti-malware software?	.765
	EU1.12	Indicate the extent to which you use each of the following items for the technology in your unit: Computers that are protected by one or more firewalls?	.763
Frequency of Use of Preventative Measures	EU2.5	Please indicate the frequency for which each of following is true for the equipment in your unit: You require authorized users to change their passwords?	.516
	EU2.6	Please indicate the frequency for which each of following is true for the equipment in your unit: You update antivirus definitions for the computers in your school or department?	.917
	EU2.7	Please indicate the frequency for which each of following is true for the equipment in your unit: You update the anti-malware settings to reflect current or emerging threats?	.925
Frequency of Use of Preventative Measures (cont.)	EU2.8	Please indicate the frequency for which each of following is true for the equipment in your unit: You update the firewall settings to reflect current or emerging threats?	.875
	EU2.9	Please indicate the frequency for which each of following is true for the equipment in your unit: You update the firewall setting to allow approved applications to access the network?	.809
	EU2.10	Please indicate the frequency for which each of following is true for the equipment in your unit: You run critical software and operating system updates on computers?	.750

Extent of Use of a Backup Policy Where Backups are Kept Offline	EU1.13	Indicate the extent to which you use each of the following items for the technology in your unit: Regular backups of servers or other vital computer resources that are then kept offline?	.731
	EU2.11	Please indicate the frequency for which each of following is true for the equipment in your unit: You back up servers or vital computer resources according to a backup policy that requires offline storage of backups?	.983
Degree of User Community Awareness of Security Issues	ED1.1	Please indicate the extent to which you feel that the user community you support is educated about the following topics related to information security: The need to update their work computer's operating system and/or applications whenever a new update becomes available?	.783
Degree of User Community Awareness of Security Issues (cont.)	ED1.2	Please indicate the extent to which you feel that the user community you support is educated about the following topics related to information security: The need to update their antivirus definitions whenever a new update becomes available?	.693
	ED1.3	Please indicate the extent to which you feel that the user community you support is educated about the following topics related to information security: The need to exercise caution when using USB drives or external hard drives, which they have previously used outside the workplace, on a school or department computer?	.833
	ED1.4	Please indicate the extent to which you feel that the user community you support is educated about the following topics related to information security: The need to exercise caution when downloading or installing software or apps from untrusted sources onto their work computers?	.839

	ED1.5	Please indicate the extent to which you feel that the user community you support is educated about the following topics related to information security: The need to exercise caution when engaging in conversations that could divulge sensitive information to unauthorized personnel, such as is common in social-engineering type situations?	.611
Degree of User Community Awareness of Security Issues (cont.)	ED1.6	Please indicate the extent to which you feel that the user community you support is educated about the following topics related to information security: The need to exercise caution when opening email attachments and clickable links in email?	.736
Perceived Awareness of the Immediate Threat Environment	PA1.1	How do you rate your level of knowledge for each of the following for the equipment in your school or department: The volume and type of network traffic that takes place on your network?	.885
	PA1.2	How do you rate your level of knowledge for each of the following for the equipment in your school or department: The nature and type of network traffic on any networks that connect with yours?	.870
	PA2.1	Rate your level of awareness for each of the following items regarding the technology in your unit: The type of network traffic on your department network?	.837
	PA2.2	Rate your level of awareness for each of the following items regarding the technology in your unit: The type of network traffic on your department network?	.767
Perceived Awareness of Vulnerabilities in the Physical Infrastructure	PA1.3	Rate your level of knowledge for each of the following items for the technology in your unit: The vulnerability of your computers and network equipment to a cyberattack?	.764
	PA1.4	Rate your level of knowledge for each of the following items for the	.832

		technology in your unit: The physical design and layout of your network?	
Perceived Awareness of Vulnerabilities in the Physical Infrastructure (cont.)	PA2.3	Rate your level of awareness for each of the following items regarding the technology in your unit: The number and severity of potential vulnerabilities on your network?	.829
	PA2.4	Rate your level of awareness for each of the following items regarding the technology in your unit: The overall physical infrastructure of your network?	.833
Perceived Awareness of Defensive Measures in Place	PA1.5	Rate your level of knowledge for each of the following items for the technology in your unit: The type of defensive measures that are currently protecting your network?	.83
	PA2.5	Rate your level of awareness for each of the following items regarding the technology in your unit: The defensive measures that protect your network?	.835
Perceived Readiness to Detect Attacks	PR1.1	Rate your ability in relation to each of the following items for the technology in your unit: To detect whether a computer or network resource has been compromised by malware?	.812
	PR1.2	Rate your ability in relation to each of the following items for the technology in your unit: To detect whether a computer or network resource is being used in support of an illegal activity such as a Distributed Denial of Service (DDoS) attack?	.903
	PR2.1	Rate your readiness to address each of the following for the equipment in your school or department: To detect whether a computer or network resource has been hacked?	.847
Perceived Readiness to Prevent Attacks	PR1.3	Rate your ability in relation to each of the following items for the technology in your unit: The vulnerability of your computers and network equipment to a cyberattack?	.906

	PR1.4	Rate your ability in relation to each of the following items for the technology in your unit: The physical design and layout of your network?	.857
	PR2.2	Rate your readiness to address each of the following for the equipment in your school or department: To prevent a ransom ware attack from limiting users' ability to access data resources?	.799
	PR2.3	Rate your readiness to address each of the following for the equipment in your school or department: To prevent a ransom ware attack from encrypting servers or sensitive data resources such as data that falls under FERPA or HIPPA regulations?	.809
Perceived Readiness to Recover From Attacks	PR1.5	Rate your ability in relation to each of the following items for the technology in your unit: To recover users' access to vital computer resources in the event of a ransom ware attack without paying the ransom?	.809
	PR2.4	Rate your readiness to address each of the following for the equipment in your school or department: To recover data resources after they have been fully or partially erased by a computer virus?	.886
	PR2.5	Rate your readiness to address each of the following for the equipment in your school or department: To recover data resources after they have been encrypted by a ransom ware?	.893

5.3 Path Model Diagram and Results

After the measurement model was validated, a path analysis that used the participants' average scores on the measurement variables to represent each factor was conducted. Table 22 lists the mean and standard deviations for all the participants' scores averaged across factors. Survey items were coded according to a Likert-type scale. All survey items were corrected prior

to analysis to correspond with the traditional format of 1 equaling “strongly disagree” and 5 equaling “strongly agree”.

Table 22: Means and Standard Deviations for averaged participants’ scores

Factor Label	Factor Description	N	Mean	S.D.
PrevExpe	Previous Experience	135	2.111	.87389
RskAvoid	Risk Avoidance	135	3.6741	.97860
NwActMon	Extent of Use of Network Activity Monitoring Activities	135	2.6741	1.19751
PhysCtrl	Extent of Use of Physical Control over Computer and Network Resources	135	3.7630	1.22364
PrvSWMea	Extent of Use of Preventative Software Measures	135	4.4617	.81343
FrPrvMeas	Frequency of Use of Preventative Measures	135	3.7272	1.22298
RgOffBck	Extent of Use of Regular Offline Backups	135	3.7889	1.33616
UsrCommA	User Community Awareness of IT Security Issues	135	3.2679	.90239
AwarThrt	Perceived Awareness of the Immediate Threat Environment	135	3.2926	1.08007
AwarVuln	Perceived Awareness of Vulnerabilities in the Physical Infrastructure	135	3.5722	1.03207
AwarDefM	Perceived Awareness of the Defensive Measures Protecting Computer Resources	135	3.6704	1.06358
PRDetect	Perceived Readiness to Detect Cyberattacks	135	3.6840	1.10202
PRPrevnt	Perceived Readiness to Prevent Cyberattacks	135	3.3685	1.05264
PRRecovr	Perceived Readiness to Recover from a Cyberattack	135	3.5926	1.14291

Figures 12 and 13 below show the full PACRM path model, first with the hypothesized relationships (Fig. 12) and then with the results (Fig. 13).

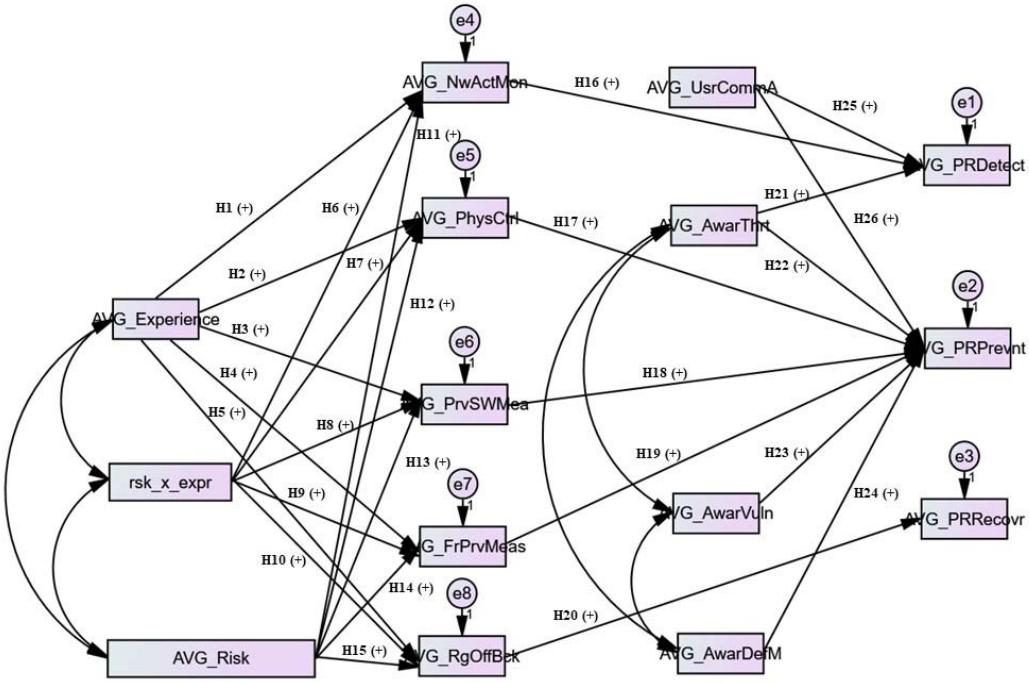

Figure 12: PACRM Path Model with Hypothesized Relationships

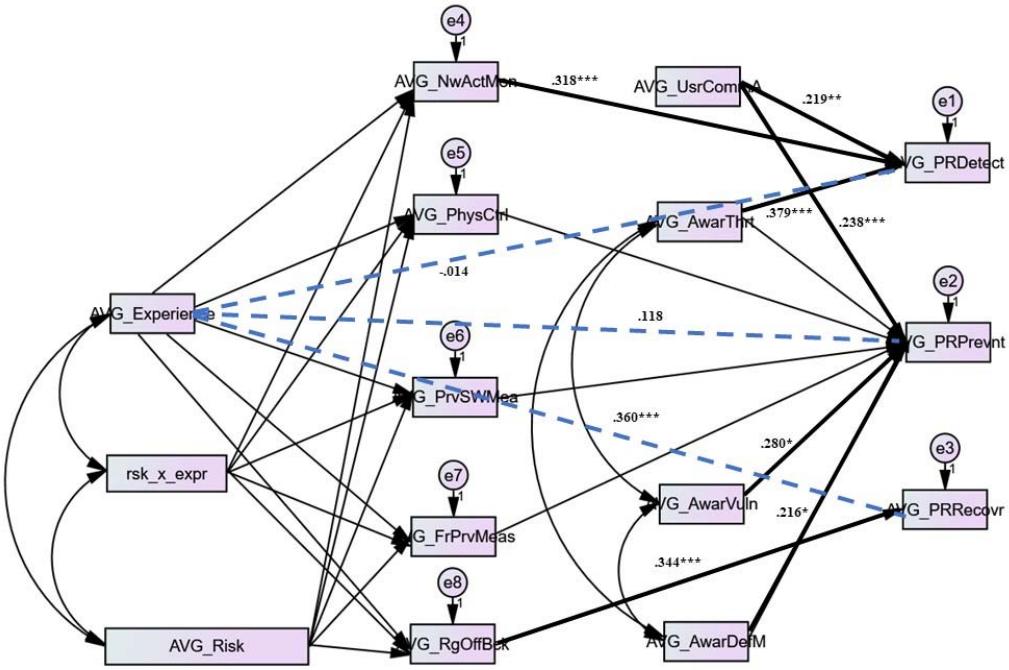

Figure 13: PACRM Path Model Results

*** denotes significance at the .001 level
** denotes significance at the .01 level
* denotes significance at the .05 level

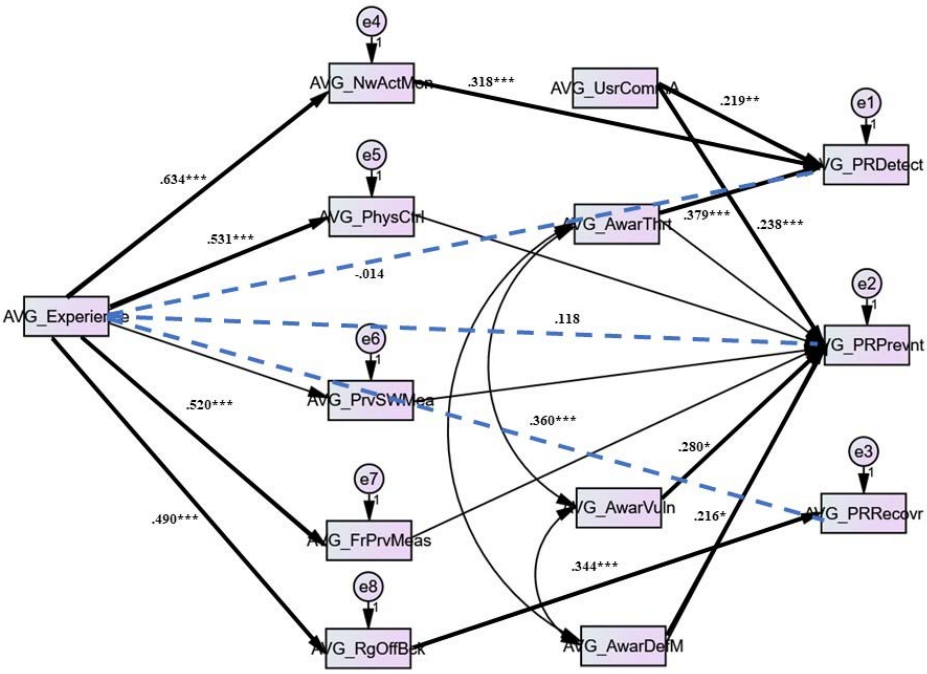

Figure 14: PACRM Path Model Results when Risk Avoidance and Interaction Term are Removed

*** denotes significance at the .001 level
** denotes significance at the .01 level
* denotes significance at the .05 level

Table 23: PACRM Path Model Results with Risk and Interaction Term Included

Hypothesis #	Regression Path	Param. Value	S.E.	Critical Value	P
H1	Experience → Network Activity Monitoring	.551	.352	1.565	.118
H2	Experience → Physical Control	.323	.372	.869	.385
H3	Experience → Prev. Software Measures	.277	.265	1.046	.296
H4	Experience → Freq. Preventative Measures	.233	.375	.622	.534
H5	Experience → Regular Offline Backups	.463	.418	1.106	.269
H6	Risk/Exp. Interaction → Network Act Mon	.020	.098	.199	.842
H7	Risk/Exp. Interaction → Physical Control	.083	.104	.794	.427
H8	Risk/Exp. Interaction → Prev. Software	-.028	.074	-.376	.707
H9	Risk/Exp. Interaction → Freq. Prev. Meas.	.074	.105	.705	.481
H10	Risk/Exp. Interaction → Reg. Offline Back.	.023	.117	.193	.847
H11	Risk → Network Activity Monitoring	-.083	.244	-.340	.734
H12	Risk → Physical Control	-.025	.258	-.095	.924
H13	Risk → Prev. Software Measures	.156	.184	.847	.397
H14	Risk → Freq. Preventative Measures	-.250	.261	-.958	.338
H15	Risk → Regular Offline Backups	.062	.291	.212	.832
H16	Network Act. Mon. → Readiness to Detect	.318	.064	4.941	<.001
H17	Physical Control → Readiness to Prevent	.042	.052	.811	.417
H18	Prev. Soft. Mea. → Readiness to Prevent	.119	.073	1.637	.102
H19	Freq. Prev. Meas. → Readiness to Prevent	.078	.051	1.509	.131
H20	Reg. Offline Back → Readiness to Recover	.344	.065	5.305	<.001
H21	Awar. Immed. Thrt → Readiness to Detect	.379	.063	5.991	<.001
H22	Awar. Immed. Thrt → Readiness to Prevent	.022	.105	.208	.835
H23	Awar. Vulnerabilities → Readiness to Prev.	.280	.130	2.151	.031
H24	Awar. Defensive Mea. → Readiness to Prv.	.216	.106	2.042	.041
H25	Usr. Comm. Aware. → Readiness to Detect	.219	.076	2.899	.004
H26	Usr. Comm. Aware. → Readiness to Prevnt.	.238	.065	3.677	<.001

5.4 Discussion

Table 24 lists the hypotheses and whether they were supported by the results of the path analysis.

Table 24: List of Hypotheses and whether they were supported with Risk and Interaction Term Included

Hypothesis #	Regression Path	Supported
H1	Experience → Network Activity Monitoring	NO
H2	Experience → Physical Control	NO
H3	Experience → Prev. Software Measures	NO
H4	Experience → Freq. Preventative Measures	NO

H5	Experience → Regular Offline Backups	NO
H6	Risk/Exp. Interaction → Network Act Mon	NO
H7	Risk/Exp. Interaction → Physical Control	NO
H8	Risk/Exp. Interaction → Prev. Software	NO
H9	Risk/Exp. Interaction → Freq. Prev. Meas.	NO
H10	Risk/Exp. Interaction → Reg. Offline Back.	NO
H11	Risk → Network Activity Monitoring	NO
H12	Risk → Physical Control	NO
H13	Risk → Prev. Software Measures	NO
H14	Risk → Freq. Preventative Measures	NO
H15	Risk → Regular Offline Backups	NO
H16	Network Act. Mon. → Readiness to Detect	YES
H17	Physical Control → Readiness to Prevent	NO
H18	Prev. Soft. Mea. → Readiness to Prevent	NO
H19	Freq. Prev. Meas. → Readiness to Prevent	NO
H20	Reg. Offline Back → Readiness to Recover	YES
H21	Awar. Immed. Thrt → Readiness to Detect	YES
H22	Awar. Immed. Thrt → Readiness to Prevent	NO
H23	Awar. Vulnerabilities → Readiness to Prev.	YES
H24	Awar. Defensive Mea. → Readiness to Prv.	YES
H25	Usr. Comm. Aware. → Readiness to Detect	YES
H26	Usr. Comm. Aware. → Readiness to Prevnt.	YES

As can be seen in Table 24, when the interaction of risk avoidance and level of previous experience with cybersecurity is included in the model, only 7 of the 26 hypothesized relationships ended up being significant at some level at or below the .05 threshold. However, as can be seen in Figure 14, when the risk factor and the associated interaction term are removed from the model, as supported by its relatively low average variance explained value from Table 17 as well as by the fact that it does not significantly contribute the model, an IT manager's level of previous experience with cybersecurity comes back into play. The beta and p values for the first five hypotheses, when risk is not included in the model, are listed below in Table 25.

Table 25: PACRM Path Model Results for H1-H5 when Risk and the Interaction Term are Removed

Hypothesis #	Regression Path	Param. Value	S.E.	Critical Value	P
H1	Experience → Network Activity Monitoring	.634	.105	6.042	<.001
H2	Experience → Physical Control	.531	.112	4.749	<.001
H3	Experience → Prev. Software Measures	.142	.079	1.792	.073
H4	Experience → Freq. Preventative Measures	.520	.112	4.629	<.001
H5	Experience → Regular Offline Backups	.490	.125	3.918	<.001

There is, therefore, evidence to suggest relationships between an IT manager's level of previous cybersecurity experience and the extent of his or her use of network activity monitoring behaviors (H1, $p < .001$), the degree to which he or she exercises physical control over computer resources (H2, $p < .001$), the frequency with which he or she updates preventative measures such as passwords, firewalls, or anti-malware software (H4, $p <.001$), and the periodic use of regular offline backups (H5, $p < .001$). While the IT manager's level of previous experience does seem to influence the frequency with which he or she updates preventative measures such as adjusting the settings on firewalls, anti-virus, or anti-malware software, it does not seem to affect the extent to which he or she uses these preventative software measures (H3, $p =.073$). This suggests that either the use of preventative software measures is ubiquitous across most of the IT managers surveyed, regardless of level of experience, or that the use of preventative software measures occurs only on a limited number of computer and network resources, but that the more experienced IT managers keep those settings updated on a regular basis.

The use of network activity monitoring devices and the frequency with which IT managers examine logs looking for signs of suspicious activity did prove to be a strong determinant of their perceived readiness to detect cyberattacks (H16, $p < .001$). This is an important consideration. One significant area of concern in organizational cybersecurity is in creating opportunities for IT administrators to regularly go through their network activity logs looking for signs of suspicious

network activity. Most administrators are far too busy or disinterested to regularly peruse network log data. As this research demonstrates, however, the dividends in terms of an increased perception of readiness to detect a cyberattack are clear. Similarly, the periodic use of offline backups was a clear determinant in administrators' perceived readiness to recover from a cyberattack (H20, $p < .001$).

The IT manager's perceived awareness of the immediate threat environment, which was operationalized as his or her knowledge and awareness of the type of network traffic that is flowing through the organizational unit's computer networks and any intersecting computer networks, was also a strong indicator of his or her perceived readiness to detect a cyberattack (H21, $p < .001$). However, the assurances provided by such knowledge did not extend to an increased perceptual readiness to prevent a cyberattack (H22, $p = .835$). This suggests that detection and prevention of cyberattacks are indeed two very distinct subsets of cybersecurity and network administrative skills and that while some IT administrators may feel well versed in the detection of suspicious activity, they do not necessarily feel as though they can prevent cyberattacks. It is important to be realistic, therefore, about the fact that, considering zero-day exploits and other non-detectable threats, prevention of cyberattacks is a very different animal than is detection.

Awareness of vulnerabilities in the physical infrastructure and awareness of defensive measures were statistically significant determinants of a perceived readiness to prevent a cyberattack (H23 & H24, $p < .05$). Recall from the discussion on discriminant validity earlier in this chapter that these two factors were highly correlated with one another. It may be that some second-order latent factor such as preparedness is driving the responses on the survey items.

Therefore, it is not entirely surprising that these variables would act upon perceived readiness to prevent a cyberattack in a similar manner.

What is particularly interesting about this research is the apparent effect that the degree to which the user community is educated on IT security issues affects the administrator's perceived readiness to detect (H25, $p < .01$) and prevent (H26, $p < .001$) cyberattacks. This is a hallmark of complex, multi-tiered, decentralized organizations. Since workgroup IT managers who work at the organizational-unit level of such institutions are often doing so in support of a small user community, this research highlights the importance of training programs to educate those users on adhering to safe computer behaviors in the workplace. Such behaviors may include not using USB drives in personal and work computers or being wary of situations in which phishing or social engineering attempts are likely to occur.

One way to conceptualize the scope of this finding is that smaller organizations, such as entrepreneurships operate in very similar ways as do individual departments within larger organizations do. A start-up business might, for example, have only one or two IT administrators who struggle with safeguarding the computer resources of the business while managing excessive demands on their time and resources. Often that person may not even have a background in IT management. By highlighting the apparent effectiveness of educating the user community on issues related to IT security, this research supports a way to increase the cybersecurity profile for such organizations. It should be clear, in fact, from the recent, high profile cyber and ransom ware attacks that have taken place that cybersecurity is an issue that affects everyone. To be sure, many behaviors, such as using network activity logging mechanisms like Intrusion Detection and Prevention Systems and sensors, as well as regularly monitoring the log data from those devices, rest squarely on the shoulders of the IT

administrator. Similarly, the periodic use of offline backups of important organizational unit data is a task that is best suited for the individual IT administrator. However, gone are the halcyon days where employees, executives, students, educators, and administrators could breathe an inward sigh of relief every time they read about a cyberattack and think to themselves, "I'm glad that I don't have to deal with that." As this research plausibly demonstrates, the behavior of the user community on issues related to IT security can positively or adversely affect IT administrators' level of comfort in their ability to detect and prevent cyberattacks. This is an especially important consideration in decentralized institutions such as colleges and universities where the local workgroup IT manager may be the sole individual responsible for securing the organizational unit's data resources.

Finally, the results from the path analysis show that only one of the direct effects between the IT administrator's level of previous cybersecurity experience and the three response variables was significant. The relationship between the IT administrator's previous cybersecurity experience and his or her perceived readiness to recover from a cyberattack was significant ($p < .001$). Similarly, previous experience in cybersecurity was a strong determinant of an IT administrator's extent of use of regular, offline backups (H5, $p < .001$), which in turn was a strong determinant of his or her perceived readiness to recover from a cyberattack (H20, $p < .001$). The fact that the direct effect was significant suggests that the relationship between an IT administrator's level of previous experience with cybersecurity and his or her perceived level of readiness to recover from a cyberattack is only partially mediated by the extent of his or her use of regular, offline backups.

In this case, the IT administrator's level of experience may be driving his or her perceived readiness to recover from a cyberattack, above the effect provided by the extent of his or her use

of regular, offline backups. This is not unreasonable since the measures related to the IT manager's behavior regarding backing up critical data were explicitly directed towards those behaviors that involved offline backups. However, IT administrators routinely keep numerous backups of critical data and only a very few (or one) of them may be kept offline. These additional backups would then, reasonably, be a determinant in the administrator's perceived readiness to recover from a cyberattack.

There was, however, a lack of a statistically significant direct effect between the IT manager's level of previous cybersecurity experience and his or her perceived readiness to detect a cyberattack, even though both indirect effects were significant (H1 & H16, $p < .001$). According to Barron & Kenny (1986), this indicates that the extent of an IT administrator's use of network activity monitoring devices fully mediates the relationship between his or her level of previous experience with cybersecurity and his or her perceived readiness to detect a cyberattack.

It is not unreasonable to conclude that the relationship between the IT administrator's level of previous experience with cybersecurity and his or her perceived readiness to detect a cyberattack is fully mediated by his or her use of network activity monitoring devices. As was commented upon in the literature review of this dissertation, detection of extant cybersecurity threats remains one of the most challenging aspects of cybersecurity to this day. The use of network activity monitoring devices such as traffic analyzers and sensor deployments greatly aid in the discovery process. One would not expect to see a high level of perceived readiness to detect cyberattacks, at any level in the organization, without the routine use of such devices.

5.5 Concluding Remarks

This research was originally undertaken to shine a light, however dim, on the darkened corner of information security research that is the higher education sector. Vast numbers of

workgroup IT managers at colleges and universities across the United States are responsible for safeguarding large territories of sensitive computer and data resources. Student admissions data or staff and faculty health data are examples that readily spring to mind. However, the work of such administrators, particularly with respect to cybersecurity, often seems to go unnoticed. Since such administrators may or may not report directly to the centralized IT department, their cybersecurity preparedness may all too often be overlooked when looking at the cybersecurity profile of the organization. To make matters worse, only a very small slice of the information security research that has taken place in recent years has looked at the higher education sector. It is heartening to note that, in the year and a half that this research has taken, more studies relating to information security in higher education have begun to emerge (Kobezak et al., 2018; Khouja et al., 2018). This is a good thing.

Since institutions of higher learning are among the most decentralized and open institutions in our society, understanding how information security can be improved upon in these settings informs us all. How should organizational cybersecurity look when there is little opportunity for rigid controls and punitive deterrents to enforce proper behaviors? In all decentralized organizations, of which colleges and universities are merely one example, it is imperative that we empower the human resources in the individual departments to engage in workplace behaviors, which this and other research studies have affirmed aid in the ability of workgroup IT managers to detect, prevent, and, if necessary, recover from a cyberattack.

6 DISCUSSION & CONCLUSION

6.1 Summary of Results

To summarize, this study examined the effects that factors related to workgroup IT managers' level of previous experience with cybersecurity, their attitudes towards risk avoidance, the extent of their use of networking and cybersecurity best practices, their awareness of several aspects of their computing and network environments, and the extent to which their user communities were educated about topics related to IT security, have on their perceived readiness to detect, prevent, and recover from a cyberattack. A new instrument, the Practice and Awareness Cybersecurity Readiness Model (PACRM) survey, was proposed and validated. As part of the instrument validation process, three distinct stages of research were conducted. Stages 1 and 2 comprised the pilot test or pre-test phase while stage 3 made up the roll-out phase. Stage 1 consisted of qualitative interviews with a handful of IT administrators working at the decentralized, department level of a large, public university in the southeastern United States. It also consisted of a "think-aloud" protocol while the administrators took a paper-based version of the initial PACRM survey. Stage 2 consisted of a pilot test whereby the PACRM survey was administered to several IT administrators at colleges and universities throughout the southeastern United States. Taken together, stages 1 and 2 helped to establish of the content validity of the PACRM instrument.

Stage 3 consisted of a national survey of 161 IT administrators working at colleges and universities throughout the United States. Reliability statistics showed good reliability for all thirteen of the proposed factors. Additionally, a Confirmatory Factor Analysis (CFA) on the refined PACRM measurement model showed a fair model fit. Lastly, a path analysis, which used participants' averaged scores on the measurement variables to represent each factor, showed that 11 of the 21 hypotheses were supported (See Tables 23 & 24).

6.2 The Motivation for the Project

As alluded to above, this project was initially undertaken to combat the relative paucity of information security research, which relates to the higher education sector. Since the principal researcher spent a time as a workgroup IT manager at several institutions of higher learning throughout the United States, this research was also undoubtedly a catharsis. Above all, it was a way to answer the question that had been bouncing around the researcher's mind for years, what are administrators in colleges and universities doing in terms of cybersecurity? It was a question that needed to be answered. Over the course of the year and a half that it took to take this project from conception to fruition, however, it has grown into something more. Through speaking and emailing with IT administrators across the country, hearing their frustrations, witnessing their overwhelming generosity in overcoming their initial suspicions to help a PhD student complete his research, a profound appreciation for the work that they do emerged. Although this country has recently been besieged by incident after incident, the evidence is suggestive that the most efficient solution, indeed the only cost-effective solution for IT administration at the decentralized level, is in raising the self-efficacy expectations of the human IT managers at organizations across the country. As any good MIS textbook will tell you, after all, the most important component of any information system is the person.

6.3 Genesis of the Conceptual Model

The primary genesis for the Practice and Awareness Cybersecurity Readiness Model came from the researcher's own experiences as a workgroup IT manager at several decentralized institutions of higher learning across the United States. During such work, it was often frustrating to realize that so much more than was being done in terms of cybersecurity could be done with only a little more time or a little more budget.

The first step in developing the model came with the awareness that the response variables in many information security studies often have very little to say about the direct, daily actions of the actual IT administrator. The first challenge, therefore, in developing the model, lay in the problem of how to conceive of IT security in a way which relates to the day-to-day actions of the IT administrator, whether he or she be at the centralized or decentralized level of IT administration. What does information security look like on the ground, as it were? The clearest answer to that question was found in the numerous and excellent standards and frameworks for good IT management, which have been published over the years by regulatory and government entities. The NIST 2014 high-level functions listed in Table 2 of this dissertation were particularly helpful in deciding on the response variables of choice depicted in Figures 1 and 6.

Secondly, the independent variables had to be chosen. It was apparent early in the conceptual design process that the model would focus on the daily practices of IT administrators as well as on more general aspects of "awareness" of the computing and networking environment in and around the organizational unit. The specific constructs that would comprise these amorphous groups had yet to be decided upon, however. Again, the international and national standards, which the United States federal government and others use to safeguard their data resources, were immensely helpful. However, also informative in this regard were the

numerous, high-quality research studies from the Management Information Systems and Computer Information Systems disciplines. The innumerable research studies on incidents of computer abuse (only a few of which made their way into this dissertation) from the early nineties from Detmar Straub and others, which are based in General Deterrence Theory, were particularly determinative in illuminating one of the many paths that information security research has taken over the past thirty years. Equally as rewarding, however, were the studies that look at information security from the vantage point of the Theory of Planned Behavior. This, of course, led to a realization that what the model had been trying to get at, all along, was how to define and increase the self-efficacy of workgroup IT managers in terms of cybersecurity. The fact that the perceived readiness of IT managers to detect, prevent, and recover from a cyberattack dovetailed so nicely with Bandura's original conception of efficacy expectations is what cemented the PACRM model's place within the Self-Efficacy Theory camp of information security research.

Lastly, the role of the IT administrator's level of previous experience with cybersecurity, as well as the role that his or her attitude towards risk played in the model had to be conceptualized. From experience and from the literature, it was decided that the IT manager's level of previous experience indelibly shaped the extent of his or her use of cybersecurity best practices, which by this point had crystallized around the use of network activity monitoring devices, control over physical access to computer resources, the use of preventative software measures, and the use of offline backups. It was the McHugh et al. article (2000) that led to the conceptualization that the level of previous experience with cybersecurity construct had to entail the dual perspectives of both cyberattack and cyber defense. Fred Kaplan's excellent book entitled, "Dark Territory: The Secret History of Cyber War," illustrates that the NSA conceptualizes cybersecurity in a

similar way, as comprising elements of both CNA (Computer Network Attack) and CND (Computer Network Defense), as well as the more nebulous third element of CNE (Computer Network Exploitation). Meanwhile, it seemed natural that an IT manager's attitude towards risk would moderate the relationship between his or her level of previous experience with cybersecurity and the extent of his or her use of networking and cybersecurity best practices.

The group of "awareness" factors came together much more slowly. It was known from the beginning of the model development process that these three factors should comprise elements that were of daily concern to IT administrators. As such, the first factor, *Awareness of the Immediate Threat Environment*, seemed fairly straightforward. The numerous articles that stressed the importance of placing network sensors on both sides of the network periphery as part of a "Defense in Depth" strategy seemed to confirm this viewpoint. As stated previously, a full strategy, requiring dozens of strategically placed sensor and traffic analyzers on both sides of the network border, would seem to be beyond the scope of many decentralized organizational units. However, a knowledgeable IT administrator, who knows the behaviors and habits of his or her user community and who frequently examines the data from a single IDS/IPS, will have an above average idea of what type of network traffic is flowing across the network without resorting to an expensive, laborious array of sensors.

Once the outward-looking construct was thus conceived, it seemed prudent to look inward at the physical infrastructure of the computer network and any vulnerabilities that may exist therein. Once vulnerabilities or other potential areas of weakness were identified, defensive measures could be deployed. Hence, the second and third awareness constructs were born. It was thought that by looking outward, towards the threats that IT administrators might face, they would feel that much more ready to detect potential cyberattacks. By looking inward, however,

at how the network was laid out and at any potential vulnerabilities as well as the defensive measures that were in place to safeguard the network, IT administrators might show a greater readiness to prevent said attacks.

Lastly, the *Degree to Which the User Community is Aware of Issues Related to IT Security* came about, as mentioned, through the qualitative interview process. It's primacy in affecting both IT administrators' perceived readiness to detect and prevent cyberattacks speaks to the efficacy and necessity of the instrument validation process.

6.4 Conclusions about the Conceptual Model

This research, which represents the first iteration of empirical testing for the PACRM model, showed that the model performed reasonably well despite several aspects of the research that can be greatly improved upon in future attempts. First, as the initial PACRM measurement model in Table 5 of this dissertation shows, the survey that was used to test the underlying theoretical assumptions was not particularly well designed. Some constructs had twelve associated measurement variables while others had only two. This poor design ultimately proved somewhat serendipitous by making it clear through the CFA process that the frequency with which the settings on software preventative measures such as firewalls, antivirus, and anti-malware software are updated does not equate with the extent of use of such software. A plausible explanation for this seeming discrepancy is that workgroup IT managers deploy such software on only a limited set of computer resources (presumably those that hold sensitive data) but that they update the settings on such software regularly. Furthermore, many of the measurements from the initial survey were not used in the final measurement model due to low factor loadings. The refined PACRM measurement model is, therefore, far more parsimonious than was the initial attempt. Nonetheless, a more well-designed survey should be developed. Doing so should

greatly improve how the model performs, both in terms of overall model fit and in terms of the discriminant validity of the proposed constructs.

Furthermore, it was evident from this analysis that the *Awareness of Vulnerabilities in the Physical Infrastructure* and *Awareness of Defensive Measures* were very closely correlated in the minds of the study's participants. Again, this might be an instance where cleaning up the measurement instrument used to test the model could be of enormous benefit.

6.5 Implications for Researchers

Taken as a whole, the Practice and Awareness Cybersecurity Readiness Model represents a theoretical basis upon which the gauge (and hopefully raise) the self-efficacy expectations of Workgroup IT managers with respect to their cyber security readiness. It provides a unified set of constructs that are grounded in the day-to-day practices of IT managers as well as in their awareness of the computing and networking environments that they oversee. Researchers will able to test how those daily practices and levels of awareness interact within different settings and under different conditions. Many of the constructs in the model are fairly specific. Researchers should therefore welcome the opportunity to pull the constituent parts of the model apart to test under what conditions they hold true. Even though the testing of this model took place within a specific context of IT administration, namely at the decentralized level of IT administration at colleges and universities, it should be equally as applicable to other levels of IT administration across a variety of organizational contexts.

Lastly, the enumeration of the three response variables in the PACRM model should hopefully help to guide future information security research towards projects in which the answers to the questions being asked are rooted in the day-to-day concerns of IT practitioners.

6.6 Limitations for Conceptual Model Validity

The model was developed using a specific, implicit set of cultural assumptions that are based in the principal researcher's many years of personal experience as a workgroup IT manager working at the decentralized level of IT administration within the United States. It was also well grounded in national and international frameworks as well as in a rich corpus of Management Information Systems and Computer Information Systems literature. Nonetheless, there is no reason to believe that the assumptions, which are intrinsic to the model, will hold true across every conceivable cultural or situational context. The model may perform very differently in other settings where, for instance, cyber defense takes on different priorities and meanings. It cannot immediately be assumed, for example, that the the values of authenticity, confidentiality, and availability, upon which the three response variables are predicated, will always have the same meaning.

6.7 Directions for Future Research

The most immediate direction for future research for the PACRM model is to test the theoretical assumptions across a variety of organizational settings, to see how specifically the relationships hold up under decentralized and centralized levels of IT administration. Since the initial empirical testing took place within the higher education sector, it would seem prudent to test the model in other business and organizational settings including regional offices of multi-national firms and national firms, entrepreneurships, non-profits, healthcare, and other governmental agencies. In addition, expanding the model in terms of some of the assumptions inherent in the *User Community Awareness* factor, such as social engineering awareness, would provide a useful contribution to the literature. Finally, it seems prudent to determine under which conditions self-efficacy-based models, such as the PACRM model, perform better or

worse against solutions that are based on other theoretical orientations, such as General Deterrence Theory.

LIST OF REFERENCES

Ajzen, I. (1991). The Theory of Planned Behavior. *Organizational Behavior and Human Decision Processes, 50*, 179-211.

Ajzen, I., & Fishbein, M. (1980). *Understanding Attitudes and Predicting Social Behavior.* Englewood Cliffs, NJ: Prentice-Hall.

Bagozzi, R. (1980). *Causal Modelling in Marketing.* New York, NY: Wiley & Sons.

Ball, L., & Harris, R. (1982). SMIS members: a membership analysis. *MIS Quarterly, 6*(1), 19-38.

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

Baron, R. M., & Kenny, D. A. (1986). The moderator–mediator variable distinction in social psychological research: Conceptual, strategic, and statistical considerations. *Journal of personality and social psychology, 51*(6), 1173.

Baroudi, J., & Orlikowski, W. (1989, March). The Problem of Statistical Power in MIS Research. *MIS Quarterly, 13*(1), 87-106.

Barts Health NHS Trust. (2017, May 19). *IT Disruption.* Retrieved from Barts Health NHS Trust: http://bartshealth.nhs.uk/media/latest-news/2017/may/it-disruption/

Bentler, P. (1990). Comparative Fit Indexes in Structural Models. *Psychological Bulletin, 107*(2), 238-46.

Bentler, P. M., & Bonett, D. G. (1980). Significance tests and goodness of fit in the analysis of covariance structures. *Psychological bulletin, 88*(3), 588.

Bentler, P. M., & Chou, C. P. (1987). Practical issues in structural modeling. *Sociological Methods & Research, 16*(1), 78-117.

Bernard, T. S., Hsu, T., Perlroth, N., & Lieber, R. (2017, September 7). *Equifax Says Attack May Have Affected 143 Million in the U.S.* Retrieved from The New York Times: https://www.nytimes.com/2017/09/07/business/equifax-cyberattack.html

Blalock, H. J. (1969). *Theory Construction: From Verbal to Mathematical Formulations.* Englewood Cliffs, NJ: Prentice-Hall.

Boss, S., & Kirsch, L. (2007). Motivating Employees to Follow Corporate Security Guidelines. *ICIS 2007 Proceedings*, (pp. 1-18).

Brancheau, J., & Wetherbe, J. (1987). Key Issues in Information Systems Management. *MIS Quarterly, 11*(1), 23-45.

Brancheau, J., Janz, B., & Wetherbe, J. (1996). Key Issues in Information Systems Management: 1994-95 SIM Delphi results. *MIS Quarterly*, 225-242.

Bromium. (2017, May 9). *Cybercriminals Are Winning: Even Security Professionals Admit to Paying Ransom and Bypassing Corporate Security*. Retrieved from Bromium:

https://www.bromium.com/company/press-releases/cybercriminals-are-winning-even-security-professionals-admit-paying-ransom.html

Browne, M. W., & Cudeck, R. (1993). *Alternative ways of assessing model fit.* Sage focus editions.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly, 34*(3), 523-548.

Campbell, D., & Fiske, D. (1959, March). Convergent and Discriminant Validation by the Multitrait-Multimethod Matrix. *Psychological Bulletin, 56*, 81-105.

Cavusoglu, H., Son, J.-Y., & Benbasat, I. (2009). Information Security Control Resources in Organizations: A Multidimensional View and Their Key Drivers.

Center for Internet Security. (2017). *CIS Controls*. Retrieved from Center for Internet Security (CIS): https://www.cisecurity.org/controls/

Churchill, G. J. (1979, February). A Pardigm for Developing Better Measuress of Marketing Constructs. *Journal of Marketing Research, 16*, 64-73.

Cohen, J. (1969). *Statistical Power Analysis for the Behavioral Sciences.* New York, NY: Academic Press.

Colton, K., Tien, J., Davis, S., Dunn, B., & Barnett, A. (1982). *Computer Crime: Electronic Fund Transfer Systems and Crime.* U.S. Department of Justice, Bureau of Justice Statistics. Washington, D.C.: U.S. Department of Justice.

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

Cook, T., & Campbell, D. (1979). *Quasi-Experimentation: Design and Analytical Issues for Field Settings.* Chicago, IL: Rand McNally.

Cronbach, L. (1951, September). Coefficient Alpha and the Internal Consistency of Tests. *Psychometrika, 16*, 297-334.

Cronbach, L. (1971). Test Validation. In R. Thorndike (Ed.), *Educational Measurement* (pp. 443-507). Washington, D.C.: American Council on Education.

D'Arcy, J., Herath, T., & Shoss, M. (2014). Understanding Employee Responses to Stressful Information Security Requirements: A Coping Perspective. *Journal of Management Information Systems*, 285-318.

Davis, F. G., & Gantenbein, R. E. (1987). Recovering from a Computer Virus Attack. *The Journal of Systems and Software, 7*(4), 253-258.

Denning, D. (1987). An Intrusion-Detection Model. *IEEE Transactions on Software Engineering*, 222-232.

Dhillon, G., & Backhouse, J. (2001). Current Directions in IS Research: Towards Socio-Organizational Perspectives. *Information Systems Journal*, 127-153.

Dickson, G., Leitheister, R., Wetherbe, J., & Nechis, M. (1984). Key Information Systems Issues for the 1980s. *MIS Quarterly, 8*(3), 135-159.

Dinev, T., Goo, J., Hu, Q., & Nam, K. (2009). User behaviour towards protective information technologies: the role of national cultural differences. *Information Systems Journal*, 1-22.

Dixon, R., Marston, C., & Collier, P. (1992). A report on the joint CIMA and IIA computer fraud survey. *Computers & Security, 11*(4), 307-313.

Ehrlich, I. (1973). Participation in Illegitimate Activities: A Theoretical and Empirical Investigation. *Journal of Political Economy, 81*(3), 521-565.

Elliott, R., Young, M. O., Collins, V. D., Frawley, D., & Temares, M. L. (1991). *Information Security in Higher Education.* Boulder, CO: CAUSE, The Association for the Management of Information Technology in Higher Education.

Fishbein, M., & Ajzen, I. (1975). *Belief, Attitude, Intention, and Behavior.* Reading, MA: Addison-Wesley.

Forcht, K. (1994). *Computer Security Management.* Course Technology Press.

Gasser, M. (1988). *Building a Secure Computer System.* Von Nostrand Reinhold.

Goodhue, D., & Straub, D. (1991). Security Concerns of System Users: A Study of Perceptions of the Adequacy of Security. *Information & Management, 20*(1), 13-27.

Grant Thornton. (2016). *The 2016 Federal CIO Survey.* Professional Services Council. Professional Services Council.

Hair, J. J., Anderson, R., Tatham, R., & Grablowsky, B. (1979). *Multivariate Data Analysis.* Tulsa, OK: PPC Books.

Hartog, C., & Herbert, M. (1986). 1985 Opinion Survey of MIS Managers: Key Issues. *MIS Quarterly, 10*(4), 351-361.

Hilkert, D., Benlian, A., Sarstedt, M., & Hess, T. (2011). Perceived Software Platform Openness: The Scale and Its Impact on Developer Satisfaction. *ICIS 2011 Proceedings* (pp. 1-20). Shanghai: Association of Information Systems (AIS).

Hoffer, J. A., & Straub, D. W. (1989). The 9 to 5 Underground: Are You Policing Computer Crimes. *MIT Sloan Management Review, 30*(4), 35-44.

Hooper, D., Coughlan, J., & Mullen, M. (2008). Structural equation modelling: Guidelines for determining model fit. *Electronic Journal of Business Research Methods, 6*(1), 53-60.

Hu, L. T., & Bentler, P. M. (1999). Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives. *Structural equation modeling: a multidisciplinary journal, 6*(1), 1-55.

International Standards Organization. (2017). *The ISO 27000 Directory*. Retrieved from ISO 27000: http://www.27000.org/index.htm

Ives, B., & Olson, M. (1984). User Involvement and MIS Success: A Review of Research. *Management Science, 30*(5), 586-603.

Ives, B., Olson, M., & Baroudi, J. (1983). The Measurement of User Information Satisfaction. *Communications of the ACM, 26*(10), 785-793.

Jarvenpaa, S., Dickson, G., & and DeSanctis, G. (1984). Methodological Issues in Experimental IS Research: Experiences and Recommendations. *Proceedings of the Fifth International Information Systems Conference*, (pp. 1-30). Tucson, AZ.

Khouja, M., Rodriguez, I. B., Halima, Y. B., & Moalla, S. (2018). IT Governance in Higher Education Institutions: A Systematic Literature Review. *International Journal of Human Capital and Information Technology Professionals (IJHCITP), 9*(2), 52-67.

Kline, R. (2005). *Principles and Practice of Structural Equation Modeling.* New York: The Guilford Press.

Kling, R. (1980). Social Analyses of Computing. *ACM Computing Surveys (CSUR), 12*(1), 61-110.

Kobezak, P., Marchany, R., Raymond, D., & Tront, J. (2018). Host Inventory Controls and Systems Survey: Evaluating the CIS Critical Security Control One in Higher Education Networks. *Proceedings of the 51st Hawaii International Conference on System Sciences.*

Kohlberg, L. (1984). *The Psychology of Moral Development.* New York: Harper & Row.

Kraemer, H., & Thiemann, S. (1987). *How Many Subjects? Statistical Power Analysis in Research.* Newbury Park, CA: Sage Publishing.

Kusserow, R. (1983). *Computer-Related Fraud and Abuse in Government Agencies.* U.S. Department of Health and Human Services.

Lee, J., & Lee, Y. (2002). A holistic model of computer abuse within organizations. *Information Management & Computer Security, 10*(2), 57-63.

Lee, S. M., Lee, S. G., & Yoo, S. (2004). An integrative model of computer abuse based on social control and general deterrence theories. *Information & Management, 41*(6), 707-718.

Lindman, H. (1974). *Analysis of Variance in Complex Experimental Designs.* WH Freeman & Co.

Loch, K., Carr, H., & Warkentin, M. (1992, June). Threats to Information Systems: Today's Reality, Yesterday's Understanding. *MIS Quarterly*, 173-186.

Lohr, S., & Alderman, L. (2017, 05 15). *The Fallout From a Global Cyberattack: 'A Battle We're Fighting Every Day'.* Retrieved from The New York Times: https://www.nytimes.com/2017/05/15/world/asia/china-cyberattack-hack-ransomware.html

Long, J. (1983). *Confirmatory Factor Analysis.* Beverly Hills, CA: Sage Publishing.

MacCallum, R. C., Browne, M. W., & Sugawara, H. M. (1996). Power analysis and determination of sample size for covariance structure modeling. *Psychological methods, 1*(2), 130.

Madnick, S. (1978). Management policies and procedures needed for effective computer security. *Sloan Management Review, 20*(1), 61-74.

Marsh, H. W., Hau, K. T., & Wen, Z. (2004). In search of golden rules: Comment on hypothesis-testing approaches to setting cutoff values for fit indexes and dangers in overgeneralizing Hu and Bentler's (1999) findings. *Structural equation modeling, 11*(3), 320-341.

Mathews, L. (2017, February 7). *2016 Saw An Insane Rise In The Number Of Ransomware Attacks.* Retrieved from Forbes: https://www.forbes.com/sites/leemathews/2017/02/07/2016-saw-an-insane-rise-in-the-number-of-ransomware-attacks/#2536853058dc

McHugh, J., Christie, A., & Allen, J. (2000). Defending Yourself: The Role of Intrusion Detection Systems. *IEEE Software*, 42-51.

Merriam-Webster. (2017, May 22). *Cybersecurity (n.d.)*. Retrieved from Merriam-Webster: https://www.merriam-webster.com/dictionary/cybersecurity

Mitnick, K., & Simon, W. (2002). *The Art of Deception: Controlling the Human Element of Security.* Indiana, IN: Wiley Publishing, Inc.

Myyry, L., Siponen, M., Pahnila, S., Vartiainen, T., & Vance, A. (2009). What levels of moral reasoning and values explain adherence to information security rules? An empirical study. *European Journal of Information Systems*, 126-139.

National Center for Education Statistics. (n.d.). *Data Tools - Locators*. Retrieved 12 12, 2017, from National Center for Education Statistics: https://nces.ed.gov/datatools/

Neumann, P. (1999). Risks of Insiders. *Communications of the ACM, 42*(12), 160.

NIST. (2014). *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0.* National Institute of Standards and Technology.

Nunnally, J. (1967). *Psychometric Theory.* New York, NY: McGraw-Hill.

Oblinger, D. G., & Hawkins, B. L. (2006). The Myth About IT Security. *Educause Review, 41*(3), 14-15.

Parker, D. (1976). *Crime by Computer.* New York: Scribner's.

Parker, D. (1981). *Computer Security Management.* Reston, VA: Reston Publishing.

Parker, D. (1983). *Fighting Computer Crime.* New York, NY: Scribner's.

Perlroth, N. (2017, June 22). *A Cyberattack 'the World Isn't Ready For'.* Retrieved from The New York Times: https://www.nytimes.com/2017/06/22/technology/ransomware-attack-nsa-cyberweapons.html

Perlroth, N. (2017, 05 13). *With New Digital Tools, Even Nonexperts Can Wage Cyberattacks.* Retrieved from The New York Times: https://www.nytimes.com/2017/05/13/technology/hack-ransomware-scam-cyberattacks.html

Perlroth, N., & Haag, M. (2017, April 29). *Hacker Leaks Episodes from Netflix Show and Threatens Other Networks.* Retrieved from The New York Times: https://www.nytimes.com/2017/04/29/business/media/netflix-hack-orange-is-the-new-black.html

Perlroth, N., Scott, M., & Frenkel, S. (2017, 06 27). *Cyberattack Hits Ukraine Then Spreads Internationally.* Retrieved from The New York Times: https://www.nytimes.com/2017/06/27/technology/ransomware-hackers.html

Perry, J. L., Nicholls, A. R., Clough, P. J., & Crust, L. (2015). Assessing model fit: Caveats and recommendations for confirmatory factor analysis and exploratory structural equation modeling. *Measurement in Physical Education and Exercise Science, 19*(1), 12-21.

Piazza, P. (2006). Security goes to school. *Security Management, 50*(12), 46-51.

Ponemon Institute, L.L.C. (2014). *2014 Cost of Cyber Crime Study: United States.* HP Enterprise Security.

Posey, C., Bennett, R., & Roberts, T. (2011). Understanding the mindset of the abusive insider: An examination of insiders' causal reasoning following internal security changes. *Computers & Security*, 486-497.

Qualtrics. (n.d.). *Qualtrics Research Core*. Retrieved 06 29, 2017, from Qualtrics: https://www.qualtrics.com/research-core/

Ransbotham, S., & Mitra, S. (2009). Choice and Chance: A Conceptual Model of Paths to. *Information Systems Research*, 121-139.

Rezgui, Y., & Marks, A. (2008). Information Security Awareness in Higher Education: An Exploratory Study. *Computers & Security, 27*(7), 241-253.

Rosenberg, E., & Salam, M. (2017, April 8). *Hacking Attack Woke up Dallas with Emergency Sirens, Officials Say.* Retrieved from The New York Times: https://www.nytimes.com/2017/04/08/us/dallas-emergency-sirens-hacking.html

Sanger, D. E., Chan, S., & Scott, M. (2017, May 14). *Ransomware's Aftershocks Feared as U.S. Warns of Complexity.* Retrieved from The New York Times: https://www.nytimes.com/2017/05/14/world/europe/cyberattacks-hack-computers-monday.html

Sapegin, A., Jaeger, D., Cheng, F., & Meinel, C. (2017). Towards a System of Complex Analysis of Security Events in Large-Scale Networks. *Computers & Security*, 16-34.

Schwartz, S. (2007). Universalism values and the inclusiveness of our moral universe. *Journal of Cross-Cultural Psychology*, 711-728.

Schweitzer, J. (1989). Virus: A Strain on the System. *Security Management, 33*(3), 17A-18A.

Sharma, S., Durand, R., & Gur-Arie, O. (1981, August). Identification and Analysis of Moderator Variables. *Journal of Marketing Research*, 291-300.

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

Siponen, M., Pahnila, S., & Mahmood, M. (2010). Compliance with Information Security Policies: An Empirical Investigation. *Computer*.

Smith, M., Wallston, K., & Smith, C. (1995). The development and validation of the Perceived Health Competence Scale. *Health Education Research*, 51-64.

Straub, D. (1986). Computer Abuse and Computer Security: Update on an Empirical Study. *Security, Audit, and Control Review, ACM Special Interest Group Journal*, 21-31.

Straub, D. (1989). Validating Instruments in MIS Research. *MIS Quarterly, 13*(2), 147-169.

Straub, D. W. (1990). Effective IS Security: An Empirical Study. *Information Systems Research, 1*(3), 255-276.

Straub, D. W., & Hoffer, J. A. (1987). *Computer Abuse and Computer Security: An Empirical Study of Contemporary Information Security Systems.* IRMIS (Institute for Research on the Management of Information Systems), Indiana University School of Business . Bloomington, IN: IRMIS (Institute for Research on the Management of Information Systems).

Straub, D., & Nance, W. (1990). Discovering and Disciplining Computer Abuse in Organizations: A Field Study. *MIS Quarterly*, 45-60.

Straub, D., & Welke, R. (1998, Dec. 1). Coping with systems risk: Security planning models for management decision making. *MIS Quarterly*, 441-469.

Swanson, M., & Guttman, B. (1996). *Generally Accepted Principles and Practices for Securing Information Technology Systems.* Gaithersburg, MD: National Institute of Standards and Technology.

Tabachnick, B. G., & Fidell, L. S. (2007). *Using multivariate statistics.* Allyn & Bacon/Pearson Education.

Thatcher, J. B., & Perrewe, P. L. (2002). An empirical examination of individual traits as antecedents to computer anxiety and computer self-efficacy. *MIS Quarterly*, 381-396.

The Associated Press. (2017, May 16). *AP Interview: Surfer Worked from Bedroom to Beat Cyberattack.* Retrieved from The New York Times: https://www.nytimes.com/aponline/2017/05/16/world/europe/ap-global-cyberattack-fighter.html

Tout, S., Sverdlik, W., & Lawver, G. (2009). Cloud Computing and its Security in Higher Education. *2009 ISECON Conference Proceedings. 26*, p. 2314. Washington, D.C.: EDSIG.

Updegrove, D., & Wishon, G. (2003). Computers and network security in higher education. *EDUCAUSE Conference Proceedings.* EDUCAUSE.

Vorhies, D. W., & Morgan, N. A. (2005). Benchmarking marketing capabilities for sustainable competitive advantage. *Journal of marketing, 69*(1), 80-94.

Ware, W. (1979, October 10). *Security Controls for Computer Systems: Report of Defense Science Board Task Force on Computer Security.* Retrieved from Rand Online: www.rand.org/pubs/reports/R609-1/R609-1.html

Warkentin, M., & Willison, R. (2009). Behavioral and Policy Issues in Information Systems Security: the Insider Threat. *European Journal of Information Systems*, 101-105.

Wheaton, B., Muthen, B., Alwin, D. F., & Summers, G. F. (1977). Assessing reliability and stability in panel models. *Sociological methodology, 8*, 84-136.

Whitman, M. (2004). In Defense of the Realm: Understanding the Threats to Information Security. *International Journal of Information Management, 24*(1), 43-57.

Whitman, M., & Mattord, H. (2016). *Principles of Information Security.* Boston, M.A.: Cengage Learning.

Xue, Y., Liang, H., & Wu, L. (2011). Punishment, justice, and compliance in mandatory IT settings. *Information Systems Research*, 400-414.

7 APPENDIX A – PACRM QUALITATIVE INTERVIEW QUESTIONS – STAGE 1

1. As an Information Technology (IT) manager working at a college or university campus, which computer and network security best practices do you consider to be the most important for an IT manager in a similar setting as yours to implement in order to maximize his or her cybersecurity readiness?

2. What aspects of network security do you consider to be the most important for an IT manager in a similar setting as yours to be aware of in order to maximize his or her cybersecurity readiness?

3. How would you rank the relative importance of an IT manager's previous level of experience with cybersecurity training in determining his or her cybersecurity readiness?

4. How would you rank the relative importance of the number and type of an IT manager's cybersecurity-related certifications in determining his or her cybersecurity readiness?

5. How would you rank the relative importance of an IT manager's attitudes towards risk, both in general terms and in terms of information security, in affecting his or her perceptions of cybersecurity readiness?

6. Please take a few minutes to look over and take the PACRM survey, which follows. Please verbalize your thoughts regarding the format, structure, ease, and applicability of the survey questions as you complete the questionnaire. Note that we will not discuss your comments or interact while you are completing the survey; however, we will discuss these afterwards to help improve the questionnaire.

8 APPENDIX B – INITIAL PACRM SURVEY INSTRUMENT – STAGE 2

Start of Block: Demographic Block

D.1 How old are you?

- ❍ 19 years or below (1)
- ❍ 20 - 24 years (2)
- ❍ 25 - 29 years (3)
- ❍ 30 - 34 years (4)
- ❍ 35 - 39 years (5)
- ❍ 40 - 44 years (6)
- ❍ 45 - 49 years (7)
- ❍ 50 - 54 years (8)
- ❍ 55 - 59 years (9)
- ❍ 60 - 64 years (10)
- ❍ 65 - 69 years (11)
- ❍ 70 years or above (12)

D.2 Are you male or female?

- ❍ Male (1)
- ❍ Female (2)

D.3 Years of Experience

	0-4 (1)	5-9 (2)	10-14 (3)	15-19 (4)	20-24 (5)	25-29 (6)	30-34 (7)	35-39 (8)	40 or above (9)
How many years of experience do you have in the Information Technology (IT) field? (1)	❍	❍	❍	❍	❍	❍	❍	❍	❍
How many years of experience do you have working in IT positions at colleges and universities? (2)	❍	❍	❍	❍	❍	❍	❍	❍	❍

D.4 What state is your current school physically located in?

_____

D.5 What is your current job title?

_____

D.6 Is your direct supervisor a member of the institution's central Information Technology (IT) department or of an academic unit?

- ❍ Central IT Department (1)
- ❍ Academic Unit (2)

D.7 Does your work primarily support faculty and staff (Academic Unit) or non-academic support staff such as the institution's human resources department, physical plant department, central administration, etc. (Support Unit).

- ❍ Academic Unit (1)
- ❍ Support Unit (2)

D.8 Please indicate your level of agreement to each of the following statements:	Strongly agree (1)	Somewhat agree (2)	Neither agree nor disagree (3)	Somewhat disagree (4)	Strongly disagree (5)
In general, I try to avoid risk whenever possible. (1)	❍	❍	❍	❍	❍
I am more comfortable accepting risk in personal matters than I am in matters pertaining to my work. (2)	❍	❍	❍	❍	❍
I am not comfortable accepting risk when it comes to the information security of my school or department. (3)	❍	❍	❍	❍	❍

End of Block: Demographic Block

Start of Block: Prior Experience Block

PE.1 Please list any cybersecurity related certifications that you currently hold? If you do not have any such certifications, please mark 0 below. Common cybersecurity certifications may include Certified Information Security Auditor (CISA), Certified Information Security Manager

(CISM), Certified Information Systems Security Professional (CISSP), Certified Ethical Hacker (CEH), etc.

_____

_____

_____

_____

_____

PE.2 Please list any other IT or professional certifications that you currently hold?

_____

_____

_____

_____

_____

PE.3 How many hours have you spent taking part in cybersecurity training? (Either as part of formalized training programs or as part of certification preparation)

- ❍ 0 - 10 hours (1)
- ❍ 10 - 50 hours (2)
- ❍ 50 - 200 hours (3)
- ❍ 200+ hours (4)

PE.4 Please indicate your level of previous experience with each of the following:

	Extensive (1)	A lot (2)	A moderate amount (3)	A little (4)	None at all (5)
Preventing or stopping cyberattacks? (1)	❍	❍	❍	❍	❍
Initiating cyberattacks? (Either as part of an advanced cybersecurity certification training program, or as a Certified Ethical Hacker, or on your own) (2)	❍	❍	❍	❍	❍

End of Block: Prior Experience Block

Start of Block: Extent of Use Block

EU.1 Please indicate the extent to which you use each of the following in your unit:	Extensively (1)	A lot (2)	A moderate amount (3)	A little (4)	None at all (5)
Network activity logging mechanisms to monitor network activity? (1)	❍	❍	❍	❍	❍
Intrusion Detection Systems (IDS) and/or Intrusion Prevention Systems (IPS) on your network? (2)	❍	❍	❍	❍	❍
A sensor deployment and/or traffic analyzer for your network? (3)	❍	❍	❍	❍	❍
Controlling unauthorized physical access to network and server resources? (4)	❍	❍	❍	❍	❍

Servers or other vital computer resources are secured in a locked room and/or server cabinet? (5)	❍	❍	❍	❍	❍
Computers that have the BIOS locked, or for which it is otherwise impossible to boot from an external device? (6)	❍	❍	❍	❍	❍
Computers with encrypted hard drives? (7)	❍	❍	❍	❍	❍
Servers or other vital computer resources with encrypted hard drives? (8)	❍	❍	❍	❍	❍
Requiring strong passwords to prevent unauthorized use? (9)	❍	❍	❍	❍	❍

Computers that are protected with antivirus software? (10)	❍	❍	❍	❍	❍
Computers that are protected with anti-malware software? (11)	❍	❍	❍	❍	❍
Computers that are protected by one or more firewalls? (12)	❍	❍	❍	❍	❍
Regular backups of servers or other vital computer resources that are then kept offline? (13)	❍	❍	❍	❍	❍

EU.2 Please indicate the frequency for which each of following is true for the equipment in your unit:	Very frequently (1)	Frequently (2)	Periodically (3)	Seldom (4)	Never (5)
You monitor general network activity logs for signs of suspicious network activity? (1)	❍	❍	❍	❍	❍
You check the probing and/or block reports from any Intrusion Detection Systems (IDS) and/or Intrusion Prevention Systems (IPS) on your network? (2)	❍	❍	❍	❍	❍

You analyze reports or data from a sensor deployment (e.g., honeypots, traffic analyzers other than your IDS/IPS, etc.) for your network? (3)	❍	❍	❍	❍	❍
Unauthorized visitors have access to server and network resources? (4)	❍	❍	❍	❍	❍
You require authorized users to change their passwords? (5)	❍	❍	❍	❍	❍
You update antivirus definitions for the computers in your school or department? (6)	❍	❍	❍	❍	❍

You update the anti-malware settings to reflect current or emerging threats? (7)	❍	❍	❍	❍	❍
You update the firewall settings to reflect current or emerging threats? (8)	❍	❍	❍	❍	❍
You update the firewall setting to allow approved applications to access the network? (9)	❍	❍	❍	❍	❍
You run critical software and operating system updates on computers? (10)	❍	❍	❍	❍	❍

You back up servers or vital computer resources according to a backup policy that requires offline storage of backups? (11)	❍	❍	❍	❍	❍

End of Block: Extent of Use Block

Start of Block: Education Block

ED.1 Please indicate the extent to which you feel that the user community you support is educated about the following topics related to information security:	Extensively (1)	A lot (2)	A moderate amount (3)	A little (4)	None at all (5)
The need to update their work computer's operating system and/or applications whenever a new update becomes available? (1)	❍	❍	❍	❍	❍
The need to update their antivirus definitions whenever a new update becomes available? (2)	❍	❍	❍	❍	❍

The need to exercise caution when using USB drives or external hard drives, which they have previously used outside the workplace, on a school or department computer? (3)	❍	❍	❍	❍	❍
The need to exercise caution when downloading or installing software or apps from untrusted sources onto their work computers? (4)	❍	❍	❍	❍	❍

The need to exercise caution when engaging in conversations that could divulge sensitive information to unauthorized personnel, such as is common in social-engineering type situations? (5)	❍	❍	❍	❍	❍
The need to exercise caution when opening email attachments and clickable links in email? (6)	❍	❍	❍	❍	❍

End of Block: Education Block

Start of Block: Perceived Awareness Block

PA.1 How do you rate your level of knowledge for each of the following for the equipment in your school or department:	Extremely knowledgeable (1)	Somewhat knowledgeable (2)	Moderately knowledgeable (3)	Somewhat not knowledgeable (4)	Not knowledgeable at all (5)
The volume and type of network traffic that takes place on your network? (1)	❍	❍	❍	❍	❍
The integrity of network traffic on any networks that intersect with yours? (2)	❍	❍	❍	❍	❍

The infection rate of the computers you support in terms of viruses and/or malware is zero? (3)	❍	❍	❍	❍	❍
The vulnerability of your computers and network equipment to a cyberattack? (4)	❍	❍	❍	❍	❍
The physical infrastructure of your network? (5)	❍	❍	❍	❍	❍
The type of defensive measures that are currently protecting your network? (6)	❍	❍	❍	❍	❍

PA.2 How do you rate your level of comfort for each of the following for the equipment in your unit:	Extremely comfortable (1)	Somewhat comfortable (2)	Neither comfortable nor uncomfortable (3)	Somewhat uncomfortable (4)	Extremely uncomfortable (5)
None of your computers or network resources are being used to support illegal activities? (1)	❍	❍	❍	❍	❍
The network traffic on any networks that intersect with your network is clean and secure? (2)	❍	❍	❍	❍	❍
The number and severity of potential vulnerabilities on your network are minimal? (3)	❍	❍	❍	❍	❍
The physical infrastructure of your network is secure from being hacked? (4)	❍	❍	❍	❍	❍

The defensive measures that are currently protecting your network are sufficient to keep your system protected from a cyberattack? (5)	❍	❍	❍	❍	❍

End of Block: Perceived Awareness Block

Start of Block: Perceived Readiness Block

PR.1 How do you rate your ability in relation to each of the following for the equipment in your school or department:	Extremely able (1)	Somewhat able (2)	Moderately able (3)	Somewhat not able (4)	Not able at all (5)
To detect whether a computer or network resource has been compromised by malware? (1)	❍	❍	❍	❍	❍
To detect whether a computer or network resource is being used in support of an illegal activity such as a Distributed Denial of Service (DDoS) attack? (2)	❍	❍	❍	❍	❍

To prevent a cyberattack from stealing sensitive information from any computer or network resource? (3)	❍	❍	❍	❍	❍
To prevent a ransom ware attack from encrypting servers or sensitive data resources? (4)	❍	❍	❍	❍	❍
To recover users' access to vital computer resources in the event of a ransom ware attack, without paying the ransom? (5)	❍	❍	❍	❍	❍

PR.2 How do you rate your readiness to address each of the following for the equipment in your school or department:	Extremely ready (1)	Somewhat ready (2)	Neither ready nor not ready (3)	Somewhat not ready (4)	Not ready at all (5)
To detect whether a computer or network resource has been hacked? (1)	❍	❍	❍	❍	❍
To prevent a ransom ware attack from limiting users' ability to access data resources? (2)	❍	❍	❍	❍	❍

To prevent a ransom ware attack from encrypting servers or sensitive data resources such as data that falls under FERPA or HIPAA regulations? (3)	❍	❍	❍	❍	❍
To recover data resources after they have been fully or partially erased by a computer virus? (4)	❍	❍	❍	❍	❍
To recover data resources after they have been encrypted by a ransom ware? (5)	❍	❍	❍	❍	❍

End of Block: Perceived Readiness Block

9 APPENDIX C – REVISED PACRM SURVEY INSTRUMENT – STAGE 3

Start of Block: Demographic Block

D.1 How old are you?

- ❍ 19 years or below (1)
- ❍ 20 - 24 years (2)
- ❍ 25 - 29 years (3)
- ❍ 30 - 34 years (4)
- ❍ 35 - 39 years (5)
- ❍ 40 - 44 years (6)
- ❍ 45 - 49 years (7)
- ❍ 50 - 54 years (8)
- ❍ 55 - 59 years (9)
- ❍ 60 - 64 years (10)
- ❍ 65 - 69 years (11)
- ❍ 70 years or above (12)

D.2 Are you male or female?

- ❍ Male (1)
- ❍ Female (2)

D.3 Years of Experience

	0-4 (1)	5-9 (2)	10-14 (3)	15-19 (4)	20-24 (5)	25-29 (6)	30-34 (7)	35-39 (8)	40 or above (9)
How many years of experience do you have in the Information Technology (IT) field? (1)	❍	❍	❍	❍	❍	❍	❍	❍	❍
How many years of experience do you have working in IT positions at colleges and universities? (2)	❍	❍	❍	❍	❍	❍	❍	❍	❍

D.4 What state is your current organization physically located in?

_____

D.5 What is your current job title?

_____

D.6 Is your direct supervisor a member of the institution's central Information Technology (IT) department or of an academic unit?

- ❍ Central IT Department (1)
- ❍ Academic Unit (2)

D.7 Does your work primarily support faculty and staff (Academic Unit) or non-academic support staff such as the institution's human resources department, physical plant department, central administration, etc. (Support Unit).

- ❍ Academic Unit (1)
- ❍ Support Unit (2)

D.8 Indicate your level of agreement to each of the following items:	Strongly agree (1)	Somewhat agree (2)	Neither agree nor disagree (3)	Somewhat disagree (4)	Strongly disagree (5)
In general, I try to avoid risk whenever possible at work. (1)	❍	❍	❍	❍	❍
I am not comfortable accepting risk in matters related to my job. (2)	❍	❍	❍	❍	❍
I am not comfortable accepting risk when it comes to the information security of my department. (3)	❍	❍	❍	❍	❍

End of Block: Demographic Block

Start of Block: Prior Experience Block

PE.1 Please list any cybersecurity related certifications that you currently hold? If you do not have any such certifications, please mark 0 below. Common cybersecurity certifications may include Certified Information Security Auditor (CISA), Certified Information Security Manager (CISM), Certified Information Systems Security Professional (CISSP), Certified Ethical Hacker (CEH), etc.

_____

_____

_____

_____

_____

PE.2 Please list any other IT or professional certifications that you currently hold?

_____

_____

_____

_____

_____

PE.3 How many hours have you spent taking part in cybersecurity training? (Either as part of formalized training programs or as part of certification preparation)

- ❍ 0 - 10 hours (1)
- ❍ 10 - 50 hours (2)
- ❍ 50 - 200 hours (3)
- ❍ 200+ hours (4)

PE.4 Indicate your level of previous experience with each of the following items:	Extensive (1)	A lot (2)	A moderate amount (3)	A little (4)	None at all (5)
Preventing or stopping cyberattacks? (1)	❍	❍	❍	❍	❍
Initiating cyberattacks? (Either as part of an advanced cybersecurity certification training program, or as a Certified Ethical Hacker, or on your own) (2)	❍	❍	❍	❍	❍

End of Block: Prior Experience Block

Start of Block: Extent of Use Block

EU.1 Indicate the extent to which you use each of the following items for the technology in your unit:	Extensively (1)	A lot (2)	A moderate amount (3)	A little (4)	None at all (5)
Network activity logging mechanisms to monitor network activity? (1)	❍	❍	❍	❍	❍
Intrusion Detection Systems (IDS) and/or Intrusion Prevention Systems (IPS) on your network? (2)	❍	❍	❍	❍	❍
Sensor deployments and/or traffic analyzers for your network? (3)	❍	❍	❍	❍	❍
Physical controls to prevent unauthorized physical access to network and server resources? (4)	❍	❍	❍	❍	❍

Locked rooms and/or server cabinets to secure servers or other vital computer resources? (5)	❍	❍	❍	❍	❍
Computers with a locked BIOS or some other way to make the computer impossible to boot from an external device? (6)	❍	❍	❍	❍	❍
Computers with encrypted hard drives? (7)	❍	❍	❍	❍	❍
Servers or other vital computers with encrypted hard drives? (8)	❍	❍	❍	❍	❍
Strong password requirements to prevent unauthorized user access? (9)	❍	❍	❍	❍	❍

Computers that are protected with antivirus software? (10)	❍	❍	❍	❍	❍
Computers that are protected with anti-malware software? (11)	❍	❍	❍	❍	❍
Computers that are protected by one or more firewalls? (12)	❍	❍	❍	❍	❍
Regular backups of servers or other vital computers that are then kept offline? (13)	❍	❍	❍	❍	❍

EU.2 Indicate the frequency for which each of following items is true for the technology in your unit:	Very frequently (1)	Frequently (2)	Periodically (3)	Seldom (4)	Never (5)
You monitor general network activity logs for signs of suspicious network activity? (1)	❍	❍	❍	❍	❍
You check the probing and/or block reports from any Intrusion Detection Systems (IDS) and/or Intrusion Prevention Systems (IPS) on your network? (2)	❍	❍	❍	❍	❍

You analyze reports or data from a sensor deployment (e.g., honeypots, traffic analyzers other than your IDS/IPS, etc.) for your network? (3)	❍	❍	❍	❍	❍
You control unauthorized access to server and network resources? (4)	❍	❍	❍	❍	❍
You require authorized users to change their passwords? (5)	❍	❍	❍	❍	❍
You update antivirus definitions for the computers in your school or department? (6)	❍	❍	❍	❍	❍

You update the anti-malware settings to reflect current or emerging threats? (7)	❍	❍	❍	❍	❍
You update the firewall settings to reflect current or emerging threats? (8)	❍	❍	❍	❍	❍
You update the firewall setting to allow approved applications to access the network? (9)	❍	❍	❍	❍	❍
You run critical software and operating system updates on computers? (10)	❍	❍	❍	❍	❍

You back up servers or vital computer resources according to a backup policy that requires offline storage of backups? (11)	❍	❍	❍	❍	❍

End of Block: Extent of Use Block

Start of Block: Education Block

ED.1 Indicate the extent to which you feel that the user community you support is educated about the following items related to information security:	Extensively (1)	A lot (2)	A moderate amount (3)	A little (4)	None at all (5)
The need to update their work computer's operating system and/or applications whenever a new update becomes available? (1)	❍	❍	❍	❍	❍
The need to update their antivirus definitions whenever a new update becomes available? (2)	❍	❍	❍	❍	❍

The need to exercise caution when using USB drives or external hard drives, which they have previously used outside the workplace, on a work computer? (3)	❍	❍	❍	❍	❍
The need to exercise caution when downloading or installing software or apps from third-party sources onto their work computers? (4)	❍	❍	❍	❍	❍

The need to exercise caution when engaging in conversations that could divulge sensitive information to unauthorized personnel, such as is common in social-engineering type situations? (5)	❍	❍	❍	❍	❍
The need to exercise caution when opening email attachments and clickable links in email? (6)	❍	❍	❍	❍	❍

End of Block: Education Block

Start of Block: Perceived Awareness Block

PA.1 Rate your level of knowledge for each of the following items for the technology in your unit:	Extremely knowledgeable (1)	Somewhat knowledgeable (2)	Moderately knowledgeable (3)	Somewhat not knowledgeable (4)	Not knowledgeable at all (5)
The volume and type of network traffic that takes place on your network? (1)	❍	❍	❍	❍	❍
The nature and type of network traffic on any networks that connect with yours? (2)	❍	❍	❍	❍	❍
The vulnerability of your computers and network equipment to a cyberattack? (3)	❍	❍	❍	❍	❍

The physical design and layout of your network? (4)	❍	❍	❍	❍	❍
The type of defensive measures that are currently protecting your network? (5)	❍	❍	❍	❍	❍

PA.2 Rate your level of awareness for each of the following items regarding the technology in your unit:	Extremely aware (1)	Somewhat aware (2)	Neither aware nor unaware (3)	Somewhat unaware (4)	Extremely unaware (5)
The type of network traffic on your department network? (1)	❍	❍	❍	❍	❍
The network traffic on any intersecting networks? (2)	❍	❍	❍	❍	❍
The number and severity of potential vulnerabilities on your network? (3)	❍	❍	❍	❍	❍
The overall physical infrastructure of your network? (4)	❍	❍	❍	❍	❍
The defensive measures that protect your network? (5)	❍	❍	❍	❍	❍

End of Block: Perceived Awareness Block

Start of Block: Perceived Readiness Block

PR.1 Rate your ability in relation to each of the following items for the technology in your unit:	Extremely able (1)	Somewhat able (2)	Moderately able (3)	Somewhat not able (4)	Not able at all (5)
To detect whether a computer or network resource has been compromised by malware? (1)	❍	❍	❍	❍	❍
To detect whether a computer or network resource is being used in support of an illegal activity such as a Distributed Denial of Service (DDoS) attack? (2)	❍	❍	❍	❍	❍
To prevent a cyberattack from stealing sensitive information from any computer or network resource? (3)	❍	❍	❍	❍	❍

To prevent a ransom ware attack from encrypting servers or sensitive data resources? (4)	❍	❍	❍	❍	❍
To recover users' access to vital computer resources in the event of a ransom ware attack without paying the ransom? (5)	❍	❍	❍	❍	❍

PR.2 Rate your readiness to address each of the following for the equipment in your school or department:	Extremely ready (1)	Somewhat ready (2)	Neither ready nor not ready (3)	Somewhat not ready (4)	Not ready at all (5)
To detect whether a computer or network resource has been hacked? (1)	❍	❍	❍	❍	❍
To prevent a ransom ware attack from limiting users' ability to access data resources? (2)	❍	❍	❍	❍	❍
To prevent a ransom ware attack from encrypting servers or sensitive data resources such as data that falls under FERPA or HIPPA regulations? (3)	❍	❍	❍	❍	❍

To recover data resources after they have been fully or partially erased by a computer virus? (4)	❍	❍	❍	❍	❍
To recover data resources after they have been encrypted by a ransom ware? (5)	❍	❍	❍	❍	❍

End of Block: Perceived Readiness Block

CURRICULUM VITAE

Thomas A. Chapman
Ph.D. Candidate in Management Information Systems
The University of Mississippi

OFFICE ADDRESS:
326 Holman Hall
University of Mississippi
University, MS 38677
[redacted]
tchapman@bus.olemiss.edu
https://www.linkedin.com/in/tachapma

HOME ADDRESS:
[redacted]
Oxford, MS 38655

[redacted]

Journal Articles:

Bain, L., Bhatnagar, N., & Chapman, T.A. (2017). How do information systems (IS) programs prepare students for entry-level occupations in the computer and IT industry? *Issues in Information Systems*, *18*(3), 78-88.

Chapman, T. A. (2016). Who's knocking at my door: developing a web service visualization tool for monitoring user account health. *Issues in Information Systems*, *17*(4), 51-57.

Refereed Conference Proceedings:

Chapman, T. A. (2018, April). *Dynamic Networks: Case Studies in Perceived Challenges and Opportunities Associated with Adopting Software-Defined Networking*. ISECON 2018 Proceedings, San Antonio, TX.

Chapman, T. A. & Bhatnagar, N. (2017, Nov.) *Shifting Perspectives: Stimulating Critical Thinking Through the Use of Virtual Reality in an IS Curriculum*. EDSIGCON 2017 Proceedings, Austin, TX.

Chapman, T. A. (2016, Nov.). *Should I Stay or Should I Go: A Measure of IT Professionals' Tendency to Engage in " Job- Hopping " within E-government Settings*. ISECON 2016 Proceedings, Pittsburgh, PA.

Chapman, T. A. (2015, Nov.). *Strength Testing the Levee: Proposed Factors Affecting Cybersecurity Preparedness for IT Professionals at Institutions of Higher Learning*. ISECON 2015 Proceedings, Orlando, FL.

Chapman, T.A. & Reithel, B.J. (2015, Aug.). *Optimizing Flow in Simulated Environments for Worker Productivity*. AMCIS 2015 Proceedings, 134.

Poster Presentations:

Chapman, T. A. (2018, April). *Factors Affecting Perceptions of Cybersecurity Readiness Among Workgroup IT Managers*. Poster presented at the 2018 Southeastern Conference (SEC) Academic Conference, Auburn, AL.

Chapman, T. A. & Reithel, B. J. (2015, Aug.). *Optimizing Flow in Simulated Environments for Worker Productivity*. ERF poster presented at 21st Americas Conference on Information Systems, Puerto Rico.

Teaching Experience Summary: Semester-Length Courses Taught

- Introduction to Management Information Systems (MIS 309) – This course serves as an introduction to information systems principles for all active undergraduate business majors at the University of Mississippi. Major themes include systems analysis, data management, and security. {Student Rating: 4.24}

- Special Topics in Journalism (JOUR 350) – This course focuses on introductory programming concepts for journalists to prepare them for careers as database and web journalists, using a combination of Python and Ruby to illustrate the concepts. {Student Rating: 5.00}

Education Summary:

Doctor of Philosophy
The University of Mississippi, 2018
-major: Management Information Systems
(dissertation area: Factors Affecting Perceptions of Cybersecurity Readiness Among Workgroup IT Managers;
dissertation committee members:
chair: Brian Reithel, Ph.D.
internal members: Anthony Ammeter, Ph.D., Bart Garner, Ph.D.
external member: John Bentley, Ph.D.

Master of Arts
Mississippi State University, 2009
-major: American History
-minor: Archaeology

Bachelor of Science
Colorado State University, 1997
-major: Computer Information Systems

Other Professional Work Experience:

- January 2015 – Present - Graduate Assistant, University of Mississippi, Oxford.

- March 2013 – January 2015 - Manager of Media Technology, University of Mississippi, Oxford MS.

- March 2011 – March 2013 - System Analyst II, University of Mississippi, Oxford MS.

- January 2009 – March 2011 – Information Technology (IT) Coordinator, Colorado Northwestern Community College, Craig CO.

- January 2007 – January 2009 – Data Manager, Mississippi State University, Starkville, MS.

- August 2005 – May 2006 – U.S. History Teacher, Forest Hill High School, Jackson, MS.

- August 2004 – May 2005 – Social Studies and English Teacher, Simmons High School, Hollandale, MS.

- May 2000 – October 2001 – Peace Corps Volunteer, Kyrgyzstan, Bishkek, Kyrgyzstan.

- January 1999 – May 2000 – Programmer Analyst II, University of New Mexico, Albuquerque, NM.

- September 1997 – January 1999 – American Management Systems, Golden, CO.

- August 1994 – May 1997 – Student Worker, Colorado State University, Fort Collins, CO.

Professional Certifications:

- May 12, 2017 – Interdisciplinary Certificate in Applied Statistics (ICAS) – University of Mississippi.

Professional Service:

- April 5 – 7, 2018 – Proceedings assistant and recruiting support for the Information Systems Education Conference (ISECON) 2018, San Antonio, TX.

- February 7, 2018 – Journal reviewer for the Journal of Cybersecurity Education, Research and Practice, Kennesaw State University, Kennesaw, GA.

- October 4 – 7, 2017 – Conference reviewer for the International Association for Computer Information Systems (IACIS) 2017 conference, Philadelphia, PA.

- August 10-12, 2017 – Conference reviewer for the 23rd Americas Conference on Information Systems (AMCIS), SIGSEC track, Boston, MA.

- November 10-12, 2016 – Conference reviewer for the Information Systems Education Conference (ISECON) 2016, Pittsburgh, PA.

- November 10-12, 2016 – Conference volunteer and session chair for the Information Systems Education Conference (ISECON) 2016, Pittsburgh, PA.

- November 5-7, 2015 – Conference reviewer for the Information Systems Education Conference (ISECON) 2015, Orlando, FL.

- November 10-12, 2016 – Conference volunteer and session chair for the Information Systems Education Conference (ISECON) 2015, Orlando, FL.

- August 13-15, 2015 – Conference volunteer for the 21st Americas Conference on Information Systems (AMCIS), Puerto Rico.

Professional Development:

- August 10 - 12, 2017 – Senior-stage track participant for the Doctoral Consortium at the 23rd Americas Conference on Information Systems (AMCIS), SIGSEC track, Boston, MA.

- August 10 - 12, 2017 – Participant in the Professional Development Symposium (PDS): Social Inclusion in Practice: Supporting Diversity, Inclusion, and Engagement in the AIS at the 23rd Americas Conference on Information Systems (AMCIS), Boston, MA.

- August 10 - 12, 2017 – Participant in the Professional Development Symposium (PDS): Incorporating Social Inclusion into Information Systems Pedagogy at the 23rd Americas Conference on Information Systems (AMCIS), Boston, MA.