

2020

UNIX Administrator Information Security Policy Compliance: The Influence of a Focused SETA Workshop and Interactive Security Challenges on Heuristics and Biases

John Palmer McConnell

Follow this and additional works at: https://nsuworks.nova.edu/gscis_etd



Part of the [Communication Technology and New Media Commons](#), [Computer Sciences Commons](#), and the [Educational Technology Commons](#)

Share Feedback About This Item

This Dissertation is brought to you by the College of Computing and Engineering at NSUWorks. It has been accepted for inclusion in CCE Theses and Dissertations by an authorized administrator of NSUWorks. For more information, please contact nsuworks@nova.edu.

UNIX Administrator Information Security Policy Compliance: The
Influence of a Focused SETA Workshop and Interactive Security Challenges
on Heuristics and Biases

by

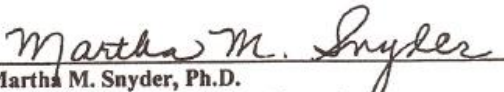
John Palmer McConnell, Jr.

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

College of Computing and Engineering
Nova Southeastern University

2020

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


Martha M. Snyder, Ph.D.
Chairperson of Dissertation Committee

11/17/2020
Date



Yair Levy, Ph.D.
Dissertation Committee Member

Nov 17, 2020
Date


Ling Wang, Ph.D.
Dissertation Committee Member

11/17/2020
Date

Approved:


Meline Kevorkian, Ed.D.
Dean, College of Computing and Engineering

11/17/2020
Date

College of Computing and Engineering
Nova Southeastern University

2020

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

UNIX Administrator Information Security Policy Compliance: The Influence of a Focused SETA Workshop and Interactive Security Challenges on Heuristics and Biases

Information Security Policy (ISP) compliance is crucial to the success of healthcare organizations due to security threats and the potential for security breaches. UNIX Administrators (UXAs) in healthcare Information Technology (IT) maintain critical servers that house Protected Health Information (PHI). Their compliance with ISP is crucial to the confidentiality, integrity, and availability of PHI data housed or accessed by their servers. The use of cognitive heuristics and biases may negatively influence threat appraisal, coping appraisal, and ultimately ISP compliance behavior. These failures may result in insufficiently protected servers and put organizations at greater risk of data breaches and financial loss. The goal was to empirically assess the effect of a focused Security Education, Training, and Awareness (SETA) workshop, an Interactive Security Challenge (ISC), and periodic security update emails on UXAs knowledge sharing, use of cognitive heuristics and biases, and ISP compliance behavior. This quantitative study employed a pretest and posttest experimental design to evaluate the effectiveness of a SETA workshop and an ISC on the ISP compliance of UXAs. The survey instrument was developed based on prior validated instrument questions and augmented with newly designed questions related to the use of cognitive heuristics and biases. Forty-two participants completed the survey prior to and following the SETA, ISC, and security update emails. Actual compliance (AC) behavior was assessed by comparing the results of security scans on administrator's servers prior to and 90 days following the SETA workshop and ISC. SmartPLS was used to analyze the pre-workshop data, post-workshop data, and combined data to evaluate the proposed structural and measurement models. The results indicated that Confirmation Bias (CB) and the Availability Heuristic (AH) were significantly influenced by the Information Security Knowledge Sharing (ISKS). Optimism Bias (OB) did not reach statistically significant levels relating to ISKS. OB did, however, significantly influence on perceived severity (TA-PS), perceived vulnerability (TA-PV), response-efficacy (CA-RE), and self-efficacy (CA-SE). Also, it was noted that all five security implementation data points collected to assess pre- and post-workshop compliance showed statistically significant change. A total of eight hypotheses were accepted and nine hypotheses were rejected.

Acknowledgements

The journey to complete my studies at NSU would not have been possible without the help of dedicated faculty, great friends, and a loving family.

First and foremost I want to thank my dissertation chair Dr. Marti Snyder. Her constant communication, direction, and support encouraged me and guided me when I needed it most. She was an awesome professor, mentor, and friend. Also critical to this dissertation was Dr. Yair Levy. It was in his security and risk class that I learned about Daniel Kahneman and the influence of cognitive heuristics on the decisions we make. Dr. Levy's direction was also key to honing the idea of how those heuristics influence UNIX administrator security compliance. Finally, Dr. Wang taught my first class and my last class at NSU. She has always provided sound guidance and advice that has been invaluable to me. I was fortunate to develop relationships with these three wonderful faculty members and they, in my opinion, truly exemplify the best in educators.

Also, instrumental in completion of my studies was my loving wife Wendy. She critiqued many papers through the years. She has also put up with many discussions about my research and never rolled her eyes or told me to go away. Her perspective, love, and encouragement made this degree possible. She cheered me on from the day I first applied to NSU. Her unfailing support has made it possible for me to dedicate a large portion of my life to my studies. My wonderful children, Kyle and Allison, have also put up with their share of discussions about my classes and their love and support have been crucial to my success.

Finally, there are several friends that I want to mention. First, is Dr. Steven Terrell, who taught me the importance of relationships. Relationships with faculty, peers, and the university are key to success in this program at NSU. Thanks also to my good friend Ali El-Sharif who became my compadre from our first meeting. We encouraged and challenged each other through the entire PhD program. Thanks also to Edward Dawson, my friend and college roommate, who endured me practicing my security workshop via Zoom many times. His feedback helped me to ensure that the workshop would be successful. Also, I need to thank my director at Johns Hopkins, Theresa Caruso. I know that I could not have completed this dissertation without her support.

Lastly, I want to thank my dad Jack and my stepmom Wanda. They taught me the value and importance of education. From my undergraduate work at Indiana University to completing this degree they have always been unfailing in their love and support.

Table of Contents

Abstract	iii
List of Tables	vi
List of Figures	ix

Chapters

1. Introduction 1

Background	1
Problem Statement	3
Dissertation Goal	6
Research Question	6
Hypotheses	7
Relevance and Significance	8
Barriers and Issues	13
Assumptions, Limitations, and Delimitations	14
Definition of Terms	14
Acronyms	16
Summary	18

2. Review of the Literature 20

Overview	20
Security Education, Training and Awareness	20
Cognitive Heuristics and Biases	27
Protection Motivation Theory	33
Information Security Policy Compliance	38
Summary	42

3. Methodology 45

Overview	45
Research Design	45
Instrument Development and Validation	54
Reliability and Validity	57
Variables	59
Population and Sampling	62
Sampling Method	64
Study Participants	65
Data Collection	66
Data Analysis	67
Format for Presenting Results	71
Resources	72

Summary	72
4. Results	74
Overview	74
Data Analysis	74
Descriptive Statistic Analysis	112
Findings	115
Summary	116
5. Conclusions, Implications, Recommendations, and Summary	118
Overview	118
Conclusions	118
Implications	123
Recommendations	124
Summary	125
Appendices	
A. Information Security Survey Form	136
B. UNIX Administrator Interactive Security Challenge	140
C. ISC Instruction Sheet	142
D. Security Update Emails	149
E. Permissions for Use of Survey Questions	161
F. Informatino Security Survey - Pilot Form	165
G. IRB Approvals	173
H. Invitation to Participate	177
I. Combined Informed Consent Form	179
References	185

List of Tables

Tables

1. Constructs and Sources	56
2. Constructs and Hypotheses	57
3. ISP Behavioral Data Points	61
4. Participant Gender	65
5. Participant Age	66
6. Participant Education	66
7. Pre-workshop Cronbach's α	77
8. Pre-workshop ρ	78
9. Pre-workshop AVE	79
10. Pre-workshop Bootstrapped AVE	79
11. Pre-workshop HTMT	80
12. Pre-workshop Inner VIF	81
13. Pre-workshop Path Coefficients	83
14. Pre-workshop Indirect Effects	84
15. Pre-workshop Specific Indirect Effects	85
16. Pre-workshop Total Effects	86
17. Pre-workshop Bootstrapped Path Coefficients	87
18. Pre-workshop Effect Size	88
19. Pre-workshop Predictive Power	89
20. Post-workshop Cronbach's α	91
21. Post-workshop ρ	92

22. Post-workshop AVE	92
23. Post-workshop Bootstrapped AVE	93
24. Post-workshop HTMT	93
25. Post-workshop VIF	94
26. Post-workshop Path Coefficients	95
27. Post-workshop Indirect Effects	96
28. Post-workshop Specific Indirect Effects	97
29. Post-workshop Total Effects	99
30. Post-workshop bootstrapped Path Coefficients	99
31. Post-workshop Effect Size	100
32. Post-workshop Predictive Power	100
33. Multigroup Cronbach's α	102
34. Multigroup ρ	103
35. Multigroup AVE	103
36. Multigroup Bootstrapped AVE	104
37. Multigroup HTMT	104
38. Multigroup VIF	105
39. Multigroup Path Coefficients	106
40. Multigroup Indirect Effects	107
41. Multigroup Specific Indirect Effects	108
42. Multigroup Total Effects	110
43. Multigroup Bootstrapped Path Coefficients	111
44. Multigroup Effect Size	112

45. Multigroup Predictive Power	112
46. Cognitive Heuristics and Biases Descriptive Statistics	113
47. Compliance T-Tests Results	115
48. Hypotheses Responses	116

List of Figures

Figures

1. Research Model 6
2. ISC Virtual Layout 53
3. SmartPLS Model Layout 70
4. Pre-workshop PLS-SEM Analysis 76
5. Post-workshop PLS-SEM Analysis 90
6. Combined Groups PLS-SEM Analysis 101
7. Cognitive Heuristics and Biases with M and σ 114
8. Compliance Metrics with M and SE 115

Chapter 1

Introduction

Background

The healthcare industry is a complicated network of hospitals, providers, independent laboratories, payers, pharmacies, imaging centers, and public health departments centered on patients and their health (Dixon, 2016). The ability to safely and efficiently store, process, and exchange information about patient care between the healthcare industry participants is key to improving patient medical outcomes and lowering the cost of healthcare (Office of the National Coordinator for Health Information Technology, n.d.; Steinbrook, 2009; Thieme, 2016). The United States federal government has encouraged the implementation of IT. The United States Patient Protection and Affordable Care Act (ACA) of 2010 provided incentives to organizations to apply technology to the healthcare system. Additionally, the American Recovery and Reinvestment Act (ARRA) of 2009 allocated \$145B for health care spending which included \$30 billion to modernize the IT infrastructure of health care organizations (Ajami & Bagheri-Tadi, 2013). Federal laws contain provisions defining the privacy and security requirements necessary to protect PHI (Steinbrook, 2009; Thieme, 2016). The goal of these laws was to encourage the use of technology to reduce healthcare costs by improving efficiency, reducing medical errors, reducing care duplication, and improving coordination of care among medical providers (Amarasingham et al., 2009; Office of the National Coordinator for Health Information Technology, n.d.). The move from paper-based health records to electronic health records (EHRs) that are shared among diverse

organizations, however, has resulted in substantially greater risk of data breaches and violations of PHI and personally identifiable information (PII) (McFarland, 2012).

While many organizations' servers are Windows based, a significant number of larger, back-end systems are UNIX based to capitalize on increased server processing power, reliability, security, and clustering technology (Bajgoric, 2006; Beuchelt, 2017a; Hussain et al., 2015). Epic and Cerner, the two leading EHR applications, represent 61% of the market for implementations in inpatient hospitals in the United States (Newman, 2019; Shrivastava, 2018). The Epic EHR application, an industry leader for hospital EHR systems, only supports UNIX based operating systems for its database and processing servers (Epic, 2018; Newman, 2019). Larger Cerner EHR customers use high-end UNIX and Linux servers for the back-end databases while many smaller hospitals may use the Windows server based version of the Cerner EHR product (Shrivastava, 2018). As of October 2020, Linux/UNIX servers represent 71.2% of all active Web servers worldwide (W3Techs, 2020). In the Amazon cloud, Linux/UNIX images represent 94% of the servers and Windows servers represent 6% of the servers out of a total of 1,368,288 images (Cloud Market, 2020). In Microsoft's Azure cloud the number of Linux virtual machines (VMs) exceeded the number of Windows VMs in 2018 (Vaughan-Nichols, 2018). When considering the total distinct known vulnerabilities from 1999 to 2020, the top six operating systems are Linux-based and Linux variants (CVE Details, 2020). As of October 2020, the top six Linux variants have 13,862 known vulnerabilities and the top four Windows operating systems have 4,865 vulnerabilities (CVE Details, 2020). Clearly, there are significant vulnerabilities with Linux and UNIX systems that need to be addressed to protect the servers that house HIPAA protected data (Caballero, 2013;

Santara, 2013).

Problem Statement

The research problem was that some UXAs fail to completely implement organizational ISP due to the use of cognitive heuristics and biases that cause them to perceive the threat of server breaches to be primarily a problem for Windows administrators (Siponen et al., 2014; Tsohou et al., 2015). This failure may leave UNIX servers open to potential systems disruption and loss of proprietary or confidential data leading to harm to organizational reputation, potential loss of revenue, or financial loss due to litigation or fines (Donaldson et al., 2015; Kraemer & Carayon, 2007). The use of OB, CB, or the AH can lead to a fundamental underestimation of risk and result in reduced ISP compliance (Pfleeger & Caputo, 2012). It is vital to understand how SETA programs, developed to address the unique job functions of UXA, influence their use of cognitive heuristics, biases, threat appraisal, and coping appraisal (Pfleeger & Caputo, 2012; Vance et al., 2012).

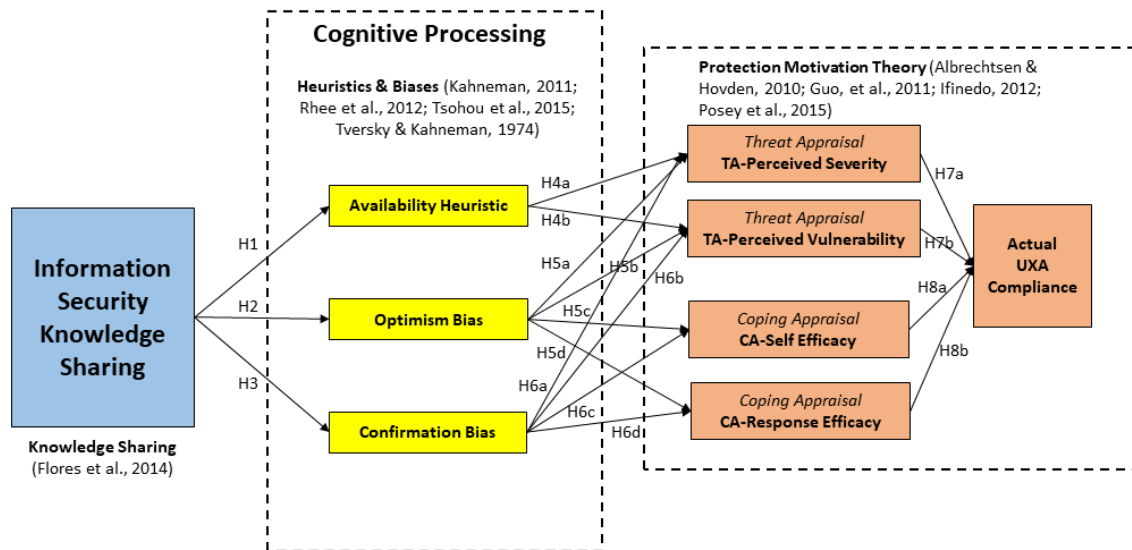
Most research in ISP compliance has focused on the end-user compliance intention (Albrechtsen & Hovden, 2010; Dang-Pham et al., 2017; Hanus & Wu, 2016; Ifinedo, 2012; Kraemer & Carayon, 2007; Safa, Von Solms, & Furnell, 2016). While end-users are critical to organizations reducing the threat of Information Security (IS) breaches, server systems administrators have the highest privilege levels and access to the vast amount of confidential PHI and PII stored on their servers (Beuchelt, 2017a; Kraemer & Carayon, 2007). Systems administrators are super users and are responsible for operating system installation, configuration, patching, user management, monitoring, data backup, implementation of security controls, disaster recovery, and testing of their

servers (Beuchelt, 2017a; Inshanally, 2018; Santara, 2013). Common IS threat vectors for servers include network, security, operating system misconfiguration, unpatched operating systems or device firmware, privileged account escalation, and unsecured data or backups (Caballero, 2013; Donaldson et al., 2015).

Human factors have gained prominence as a significant risk factor for information systems security (Bauer & Bernroider, 2017; Colwill, 2009; Ifinedo, 2014; Ki-Aries & Faily, 2017; Safa et al., 2015). To strengthen the human aspect of IS, ISPs are developed by organizations, which enhance security, decrease vulnerability to security breaches, and ensure legal compliance (Bauer & Bernroider, 2017; Bélanger et al., 2017; D'Arcy & Lowry, 2019; Furnell & Clarke, 2012; Ng, Kankanhalli, & Xu, 2009). Unfortunately, researchers have found that employees frequently circumvented information systems policies when workload increased (Albrechtsen & Hovden, 2010; Guo et al., 2011; Kraemer & Carayon, 2007) or when they felt the information systems policies were a nuisance or perceived to be irrelevant to them (Renaud, 2012; Sedighi et al., 2016). Siponen et al. (2014) identified employee failure to follow ISPs as a key threat to the security of an organization. An additional risk is that employees can make errors due to cognitive limitations, task demands, as well as organizational, social, or environmental factors (Dismukes et al., 2007; Ki-Aries & Faily, 2017; Safa & Von Solms, 2016). Most of these studies have evaluated end-user ISP compliance intention. Behavioral compliance of UXAs, however, can be even more crucial as the data housed on the back-end UNIX servers frequently contains PHI, PII, financial data, or intellectual property (Beuchelt, 2017a; Kraemer & Carayon, 2007).

IS knowledge is frequently scattered throughout organizations and many

organizations have not developed an effective ISKSprogram (Belsis et al., 2005; Flores et al., 2014; Safa & Von Solms, 2016). Additionally, organizational silos, where there is a rigid functional division between teams, can negatively impact social interaction and knowledge sharing (Oparaocha, 2016). The most effective way of increasing security knowledge sharing, and cyber skills is through effective SETA programs (Oltsik, 2017). Wash and Cooper (2018) found SETA programs to be the most effective means of changing the security behaviors of end-users. Bauer and Bernroider (2017), in assessing the impact of IS awareness on end-user compliance behavior, found that security awareness significantly positively influenced attitude toward compliance and provided a weak negative relationship to neutralizing behaviors. These studies have been limited to the effectiveness of SETA programs on ISP compliance of end-users. Although ISP compliance of UXA is crucial to protecting the organization's data, it appears very little attention was provided in the literature review on the effectiveness of focused SETA workshops that target UXA specific job functions and how the workshops influence ISP compliance behavior.

Figure 1*Research Model*

The proposed research model, based on the literature review, can be found in Figure 1. It integrates the security knowledge sharing portion of the Information Security Organizational Knowledge Sharing Framework (Flores et al., 2014), cognitive heuristics and biases (Kahneman, 2011; Rhee et al., 2012; Tsohou et al., 2015; Tversky & Kahneman, 1974), and Protection Motivation Theory (PMT) (Albrechtsen & Hovden, 2010; Guo et al., 2011; Ifinedo, 2012; Posey et al., 2015).

Dissertation Goal

The goal was to empirically assess the effect of a focused SETA workshop, an ISC, and periodic security update emails on UXAs' knowledge sharing, use of cognitive heuristics, biases, threat appraisal, coping appraisal, and ISP compliance behavior.

Research Question

The following research question guided the investigation:

How do a focused SETA workshop, ISC, and periodic security update emails designed for

UXAs, influence their ISKS, use of cognitive heuristics and biases, and ISP compliance behavior?

Hypotheses

The following hypotheses were tested:

H1: Formal knowledge sharing arrangements, in the form of a focused SETA workshop and ISC, will have a significant negative influence on UXAs' use of the AH.

H2: Formal knowledge sharing arrangements, in the form of a focused SETA workshop and ISC, will have a significant negative influence on UXAs' use of OB.

H3: Formal knowledge sharing arrangements, in the form of a focused SETA workshop and ISC, will have a significant negative influence on UXAs' use of CB.

H4a: The AH will have a significant negative influence on UXAs' IS TA-PS.

H4b: The AH will have a significant negative influence on UXAs' IS TA-PV.

H5a: OB will have a significant negative influence on UXAs' IS TA-PS.

H5b: OB will have a significant negative influence on UXAs' IS TA-PV.

H5c: OB will have a significant positive influence on UXAs' IS CA-SE.

H5d: OB will have a significant positive influence on UXAs' IS CA-RE.

H6a: CB will have a significant negative influence on UXAs' IS TA-PS.

H6b: CB will have a significant negative influence on UXAs' IS TA-PV.

H6c: CB will have a significant positive influence on UXAs' IS CA-SE.

H6d: CB will have a significant positive influence on UXAs' IS CA-RE.

H7a: UXAs security TA-PS will have a significant positive influence on UXAs' ISP compliance behavior.

H7b: UXAs security TA-PV will have a significant positive influence on UXAs' ISP compliance behavior.

H8a: UXAs' security CA-RE will have a significant positive influence on their ISP compliance behavior.

H8b: UXAs' security CA-SE will have a significant positive influence on their ISP compliance behavior.

Relevance and Significance

In 2019, in the United States the average cost of a single data breach was \$8.19 million, which included the costs of detection, notification, response, fines, litigation, and lost customer revenue (Ponemon Institute, 2019). In 2018, Health Insurance Portability and Accountability (HIPAA) penalties and settlements levied on 18 healthcare systems and insurance companies totaled \$13,501,400 (HIPAA Journal, 2020). Given the potential financial liabilities associated with data breaches and privacy violations it is imperative that healthcare organizations secure their computing resources by following the HIPAA and Health Information Technology for Economic and Clinical Health (HITECH) guidelines.

From November 2017 to October 2020 66,707,070 patient records have been breached in 50 states and the District of Columbia impacting physician practices, health plans, and hospitals (U.S. Department of Health and Human Services Office for Civil Rights, 2020). During the same period, server related incidents resulted in the loss of 50,270,087 individual's PHI records (U.S. Department of Health and Human Services

Office for Civil Rights, 2020). Server related incidents were due to hacking and IT incidents (89.7%), unauthorized access and disclosure (10.2%), and theft/loss/improper disposal (<1%) (U.S. Department of Health and Human Services Office for Civil Rights, 2020). Server breaches were responsible for 75.4% of all healthcare PHI breaches from November 2017 to October 2020 (U.S. Department of Health and Human Services Office for Civil Rights, 2020). These statistics demonstrate the importance for server administrators to consistently follow organizational ISP to ensure the confidentiality, integrity, and availability of healthcare systems, and the PII, and PHI contained therein.

The complexity of the U.S. healthcare industry's technology infrastructure, and the push toward widespread electronic sharing of PII/PHI, make securing servers and data crucial (Dixon, 2016; Office of the National Coordinator for Health Information Technology, n.d.; Steinbrook, 2009; Thieme, 2016). The HIPAA Security Rule provided specifications and standards that covered entities should implement to help ensure the confidentiality, integrity, and availability of PHI (Koch, 2017). Three categories of safeguards including physical, administrative, and technological were defined to direct organizations in how best to protect PHI (Avancha, Baxi, & Kotz, 2012). Administrative safeguards include policies, procedures, and administrative actions related to security management, vulnerability and risk assessment, workforce security training, incident reporting, and contingency planning (Koch, 2017). Physical safeguards include facility access controls, computer controls, and device and media security controls (Avancha et al., 2012). Technical safeguards include access controls, audit controls, integrity management, authentication, and transmission controls for PHI (U.S. Department of Health and Human Services, 2013). Both the Privacy and Security Rules also outline civil

and criminal penalties for the privacy violations (McFarland, 2012). These policies and guidelines, however, will not protect PII/PHI data if they are not properly implemented within the technical infrastructure (Dixon, 2016; Office of the National Coordinator for Health Information Technology, n.d.). Employees are frequently considered the weakest link in the IS chain (Furnell & Clarke, 2012; Gardner & Thomas, 2014).

Cognitive heuristics are mental shortcuts that individuals use to quickly assess a situation and determine an adequate, though frequently flawed, conclusion (Kahneman, 2011). Cognitive biases describe how information framing and context may influence decision making, which departs from normal rational theory (Gilovich & Griffin, 2013). The influence of heuristics and biases on decision making has been studied in many contexts; however, their use in the IS research has been minimal. There are a number of heuristics and biases that may negatively impact threat appraisal and coping appraisal including the AH, OB, the representativeness heuristic, the affect heuristic, and CB (Kahneman, 2011; Pennycook et al., 2013; Tsohou et al., 2015; Tversky & Kahneman, 1974). Use of these biases can result in inappropriately low judgment of risks and vulnerabilities as well as over inflated estimation of coping skills (Kahneman, 2011; Tsohou et al., 2015; Tversky & Kahneman, 1974). With the proliferation of UNIX servers, understanding and addressing the cognitive heuristics and biases used by UXAs may improve security awareness, enhance cyber skills, and increase compliance behavior thereby reducing healthcare organizations' potential for data breaches.

PMT was developed by Rogers (1975) to understand how fear appeals influenced health behaviors of patients. Rogers (1975) theorized that environmental and intrapersonal sources of information influenced the decisions people make regarding their

health. PMT is frequently used to understand compliance with ISPs and security procedures (Hanus & Wu, 2016; Safa et al., 2015; Siponen et al., 2014). Coping appraisal is an assessment of how the individual can cope with, adapt to, and change behavior to avoid danger (Rogers & Prentice-Dunn, 1997). The factors related to coping appraisal include an individual's CA-SE and CA-RE (Posey et al., 2015). CA-RE is an evaluation of the effectiveness of the proposed behavior to reduce the probability of the negative event (Rogers & Prentice-Dunn, 1997). CA-SE is the belief that one is capable of the adaptation necessary to mitigate the negative event (Rogers & Prentice-Dunn, 1997). Fear influences the evaluation of severity and vulnerability and indirectly influences behavioral intention (Rogers & Prentice-Dunn, 1997). Siponen et al. (2014) found perceived threat severity and TA-PV to be positively correlated with ISP compliance intention. Rogers and Prentice-Dunn (1997) noted that there are numerous cognitive heuristics and biases that can influence both appraisal processes in the PMT model. UXAs may perceive server threats as Windows problems leading to inappropriately low threat appraisal and excessively high coping appraisal. These erroneous cognitive assessments may lead UXAs to resist ISP implementation on UNIX servers leaving their organizations at considerable risk.

Posey et al. (2015) investigated the impact of SETA programs on PMT. SETA was positively correlated with both perceived threat severity and perceived CA-RE indicating that SETA programs are an effective way of encouraging secure behaviors (Posey et al., 2015). Appropriately designed SETA programs can help reduce the human IS risk to organizational assets (Van Vuuren, 2016; Whitman & Mattord, 2012). Although organizations spend considerable money on IS technology, users are still a major source

of failures that result in IS breaches costing organizations substantial financial loss (Safa et al., 2016). The human aspects of IS must be understood to reduce the risk of IS breaches (Van Vuuren, 2016). Users' ignorance, apathy, resistance, and mischievous nature can result in human error and cause IS breaches (Bélanger et al., 2017; Safa et al., 2016). Compliance with ISP can help to mitigate IS risk (Ifinedo, 2014). Unfortunately, employee's noncompliance with ISP is "the key threat" for organizational IS (Siponen et al., 2014, p. 217). Given the vulnerability of organizational data and the significance of human behavior in protecting data, developing an understanding of what factors encourage and discourage ISP compliance behavior will help to protect organizations (Bélanger et al., 2017; Carlton & Levy, 2015; Van Vuuren, 2016).

It can be challenging to evaluate actual ISP compliance given the risk of social desirability bias that can occur in interviews and self-reported surveys (Redmiles et al., 2017). There are techniques that can be used to remove the focus on the participant such as scenarios, which may provide better insight into non-conforming behavior (Crossler et al., 2013). When evaluating intention to perform security behaviors, researchers are challenged to determine if participants have responded with over or under-reported counts as compared to actual behaviors (Egleman & Peer, 2015). Given these risks, the present research studied actual secure behaviors rather than relying on self-reported intention to comply (Crossler et al., 2013). Developing a model that integrates SETA knowledge sharing, cognitive heuristics, and biases, and PMT provided insight into the effectiveness of a focused SETA workshop and ISC in improving UX A ISP compliance behavior.

This research helped fill the gap on SETA program development and effectiveness

with UXA. Additionally, the effectiveness of an ISC was assessed to evaluate the impact on UXA ISP compliance behavior. Finally, this study investigated actual UXA ISP compliance behavior by evaluating key server security changes made by the administrators to their UNIX servers. These checks were done by running security checks on the servers. Boss et al. (2015) also found that intention differed significantly from actual implementation of security controls. Using security scans of security measures implemented by UXA following the SETA workshop and ISC afforded unique insights into the effectiveness of the training in terms of actual implementation of security controls and ISP compliance behavior. This research was needed as implementing mandated security and compliance with organization ISP is key to the successful protection of healthcare organizational assets, including patient PHI and PII (Koch, 2017; Ng et al., 2009).

Barriers and Issues

There are several barriers and issues that were addressed. First, establishing access to the UNIX servers for the baseline security metrics was challenging due to the limitations placed on root logins and accessing servers not owned by the researcher. Ultimately, many data points were successfully collected using the tools made available by the security team (i.e. Tenable, Splunk). For other metrics scripting was used to gather evaluated data points for each administrator's servers. Second, engaging participation of the UXAs dispersed throughout the organization was challenging. Including the CISO, however, may mitigated this risk. Additionally, contacting the UXAs managers to advise them of the coming workshop and the potential benefits to their UXAs and the organization was helpful. Third, care was needed to be taken to minimize the resource

impact of scans and scripts run on servers. To minimize impact, scans and scripts were performed after hours and only after sufficient testing was completed to establish the server performance impact.

Assumptions, Limitations, and Delimitations

The following were assumptions for the present research:

- Study participants participated in the workshop, ISC, and read the periodic security update emails.
- Participants answered pre-experiment and post-experiment survey questions honestly.

The following are the limitations for the present research:

- The study was conducted in a single healthcare institution in the mid-Atlantic region of the US.
- Males represented the majority of participants (97.6%).
- The population size of 60 UXA was very small. Only 42 individuals completed all of the study protocols.

Definition of Terms

The following definitions are for terms used in the present research:

Cognitive biases—Cognitive processes that allow individuals to make seemingly flawed decisions, which depart from normative rational theory of decision making (Gilovich & Griffin, 2013).

Confidentiality—The property that ensures that information is not made available without the explicit permission or authorization from the information owner (Committee on National Standards, 2010).

Coping appraisal—A self-assessment of how an individual can cope with, adapt to, and change behavior to avoid some danger (Rogers & Prentice-Dunn, 1997). The factors related to coping appraisal include an individual's CA-SE and CA-RE (Posey et al., 2015).

Cybersecurity—The ability to protect cyberspace from potential cyber threats and attacks (Committee on National Standards, 2010).

Cyberspace—The total of the global computing infrastructure including computing devices, the Internet, telecommunications devices, controllers, and embedded computing mechanisms (Committee on National Standards, 2010).

Cognitive heuristics—Mental short cuts used to make inferences about situations (Gilovich & Griffin, 2013; Kahneman, 2011). The use of heuristics reduces cognitive load by eliminating the consideration of all causally relevant data (Kahneman, 2011; Toplak et al., 2011).

Integrity—A property defining prevention of unauthorized modification of an entity (Committee on National Standards, 2010).

Interactive Security Challenge—An online, interactive, security exercise running in a Linux VM with the goal of developing specific cybersecurity skills.

Risk—A measure of the probability (likelihood) and impact (organizational functional, reputation, mission, assets, individuals) of a potential event on an organizational asset (Committee on National Standards, 2010; Meyers & Jernigan, 2018).

Security controls—The technical, operational, and management safeguards defined to protect the integrity, confidentiality, and availability of an information system (Committee on National Standards, 2010).

Systems administrator—Users with the highest privilege levels on servers that are responsible for operating system installation, configuration, patching, user management, monitoring, data backup, implementation of security controls, disaster recovery, and testing (Inshanally, 2018; Santara, 2013).

Threat—An action that can be taken by a threat actor against a vulnerability (Meyers & Jernigan, 2018). Any event that can negatively impact an organization's operation or components in an organization (people or property) or nation by destruction, modification, or unauthorized access (Committee on National Standards, 2010).

Threat appraisal—An assessment of risk which includes the positive factors of extrinsic and intrinsic rewards offset by negative factors of the perceived severity and TA-PV to potential threats (Posey et al., 2015; Rogers & Prentice-Dunn, 1997).

UNIX—An interactive, highly portable, multiuser operating system developed by AT&T (Ritchie & Thompson, 1978).

Vulnerability—A weakness in a computing asset that can be acted upon by a threat (Meyers & Jernigan, 2018). Weaknesses can occur in procedures, processes, controls, information systems, or implementations (Committee on National Standards, 2010).

Acronyms

The following acronyms are used in the present research:

AC-Actual Compliance

ACA-Affordable Care Act

AH-Availability Heuristic

ARRA-American Recovery and Reinvestment Act

CA-RE-Coping Appraisal-Response Efficacy

CA-SE-Coping Appraisal-Self-Efficacy

CB-Cognitive Bias

CET-Cognitive Evaluation Theory

CRT-Cognitive Reflection Test

CTF-Capture the Flag

CVE-Common Vulnerabilities and Exposures

CVSS-Common Vulnerability Scoring System

EHRs-Electronic Health Records

HIPAA-Health Insurance Portability and Accountability

HITECH-Health Information Technology for Economic and Clinical Health

HTMT-Heterotrait-Monotrait Ratio

IS-Information Security

ISC-Interactive Security Challenge

ISKS-Information Security Knowledge Sharing

ISP-Information Security Policy

ISRMP-Information Security and Risk Management Plan

IT-Information Technology

NIST-National Institute of Standards and Technology

NVD-National Vulnerability Database

OB-Optimism Bias

PHI-Protected Health Information

PII-Personally Identifiable Information

PLS-SEM-Partial Least Squares Structural Equation Modeling

PMT–Protection Motivation Theory

PWC-Privacy Rights Clearinghouse

SETA–Security Education, Training, and Awareness

TA-PS-Threat Appraisal-Perceived Severity

TA-PV-Threat Appraisal-Perceived Vulnerability

TRA-Theory of Reasoned Action

UXA-UNIX Administrator

VIF-Variance Inflation Factor

VMs–Virtual Machines

Summary

UNIX servers, like their Windows counterparts, are vulnerable to IS breaches (CVE Details, 2020). Organizations are at substantial risk if employees do not follow ISPs and breaches occur (HIPAA Journal, 2020; Ponemon Institute, 2019; Yoo et al., 2018). The use of cognitive heuristics and biases can negatively impact threat appraisal and coping appraisals (Kahneman, 2011; Tversky & Kahneman, 1974). Being blind to actual risks facing their servers can result in insufficiently protected UNIX servers due to failure to comply with ISPs (Albrechtsen & Hovden, 2010; Ki-Aries & Faily, 2017; Renaud, 2012). While generalized SETA programs are useful in organizations for staff-wide training, developing a focused SETA program, ISC, and security update emails aimed specifically for the job tasks of UXA, improved engagement and ISP compliance (Chen et al., 2018; Ki-Aries & Faily, 2017). Additionally, this research helped to develop an understanding of how the SETA program, ISC, and security update emails influenced UXA use of the AH, OB, and CB. Finally, by having performed security checks prior to

and following the SETA program, ISC, and security update emails, a true indication of ISP compliance behavior was evaluated.

Chapter 2

Review of the Literature

Overview

Flores et al. (2014) as well as Albrechtsen and Hovden (2010) emphasized the importance of knowledge sharing processes in organizations. SETA workshops and online training provide formal means of ISKS within organization (Safa & Von Solms, 2016). These processes provided a starting point for the present research's cognitive model of ISP compliance. Security knowledge sharing processes are theorized to directly influence the three studied cognitive heuristics and biases used by the UXA (Kahneman, 2003; Pennycook et al., 2013). Heuristics and biases influence threat appraisal and coping appraisal from PMT (Kahneman, 2011; Pachur et al., 2012; Rhee et al., 2012; Rogers & Prentice-Dunn, 1997; Tsohou et al., 2015). The key components of PMT, threat appraisal and coping appraisal, are significantly influenced by SETA programs and are therefore critical to research into ISP compliance (Safa et al., 2016). Finally, threat appraisal and coping appraisal influence UXA compliance behavior (Safa et al., 2016). The four key areas of study for this research include: SETA; heuristics and biases; PMT; and ISP compliance behavior. These four areas can help to develop a combined cognitive behavioral theory that can help understand the factors that influence UXA ISP compliance behavior.

Security Education, Training and Awareness

SETA programs are a means for organizations to minimize the risk of insider caused security failures (Burns et al., 2015; Ki-Aries & Faily, 2017). SETA programs are

an important antecedent and positively influence IS behavior, and appropriately designed SETA programs can help reduce the human IS risk to organizational assets (D'Arcy et al., 2009; Whitman & Mattord, 2012). Users are the weakest link for IS and SETA programs can help to reduce the potential attack surface of organizations by improving the ability of users to identify and prevent IS breaches (Furnell & Clarke, 2012; Gardner & Thomas, 2014). Engaging and audience appropriate SETA programs positively influences IS CASE and ISP compliance (Chen et al., 2018; Ifinedo, 2014; Ki-Aries & Faily, 2017). Effective SETA programs should increase awareness of organizational ISP, individual responsibilities, security risks, vulnerabilities as well as potential system monitoring and sanctions (Chen et al., 2018; D'Arcy et al., 2009). Generalized SETA programs, while helping to improve security conscience behavior, may not be as beneficial for highly technical server systems administrators (Ki-Aries & Faily, 2017). Additionally, general SETA programs may not address specific security behaviors that are unique and crucial to server administrators (Ki-Aries & Faily, 2017). Schroeder (2017) found that customized security training programs improved engagement and information retention. Tailoring SETA to the job responsibilities of the participants is key to a successful and well-received program (Herold, 2011).

The sharing of IS knowledge, experience, and insights can improve organizational performance and help to ensure the security of data (Safa & Von Solms, 2016). Development of a formal means for ISKS can help to foster sharing of ideas, experiences, tools, and processes to improve security and protect an organization's information systems assets (Flores et al., 2014). Making users aware of the current and evolving IS risks, threats, vulnerabilities, and their severities, the speed with which the threats

propagate, and the potential impact to the organization is crucial to ISP compliance (Guo et al., 2011; Safa et al., 2016; Siponen et al., 2014). Dang-Pham et al. (2017) found that security awareness also improved the diffusion of IS practices (knowledge sharing) throughout the organization. Safa and Van Solms (2016) found that ISKS benefitted business, increased employee IS CA-SE, and improved ISP compliance.

The development of an ISKS culture is an important goal for any organization that has critical information systems assets (Flores et al., 2014; Razmerita et al., 2016; Safa & Van Solms, 2016). End-user education is important and developing knowledge sharing processes that include the IS team and UXA is crucial to any organization that has UNIX servers hosting business critical data (Bauer et al., 2017). It is beneficial to build both formal and informal knowledge sharing networks within organizations as they have been found to be significant contributors to awareness and mitigation of IS risks (Dang-Pham et al., 2017; Safa & Von Solms, 2016; Yoo et al., 2018). Encouraging relationships between employees across team boundaries is also helpful to developing and enabling an effective social network that fosters knowledge sharing (Bauer et al., 2017; Ifinedo, 2014; Oparaocha, 2016). Connelly and Zweig (2015) found that distrust was a predictor of knowledge hiding behaviors, which are detrimental to effective knowledge sharing in organizations. Consequently, it is important to encourage trusting relationships between the IS team and the UXA for an effective ISKS culture (Dey & Mukhopadhyay, 2018; Rutten et al., 2016).

Posey et al. (2015) found that SETA programs were positively correlated with both perceived threat severity and CA-RE indicating that they are an effective way of encouraging IS behavior and ISP compliance. SETA programs should be updated due to

the dynamic nature of IS threats and vulnerabilities (Posey et al., 2015). Yoo et al. (2018) found that the psychological flow factors including feedback, immersion, challenge, autonomy, and social interaction significantly improved psychological ownership and SETA program effectiveness. Yoo et al. (2018) suggested using relatable security scenarios that challenged employees could improve ownership and ISP compliance.

Bauer et al. (2017), in a study of ISP compliance at banks, found that developing a comprehensive, multi-modal IS awareness program was key to successfully establishing an IS culture in an organization. The goal of their research was to define specific propositions that could be used by IS management in banks to establish and maintain an effective IS awareness (ISA) program (Bauer et al., 2017). Also, Bauer et al. (2017) sought to develop an understanding of how users' perceptions of the ISA program influence their ISP compliance. The three banks studied had implemented ISA programs but with very different processes and procedures (Bauer et al., 2017). The most successful bank, in terms of IS awareness and employee engagement, conducted regular ISA campaigns using different modalities, which encouraged high levels of interaction and dissemination of critical security knowledge (Bauer et al., 2017). Bauer et al. (2017) found that some individuals used different neutralizing behaviors to justify ISP non-compliance. The third bank Bauer et al. (2017) studied had just begun an ISA program and provided little insight into SETA effectiveness. Two primary areas of design for ISA were proposed by Bauer et al. (2017): structural design and communicational design. Recommendations relevant to this study include customizing the ISA programs toward the recipients and driving for two-way discussions about IS (Bauer et al., 2017). Bauer et al. (2017) demonstrated the need for collaborative education using multiple formats to

help improve security awareness and compliance. This is relevant to the present study as it builds the foundation for the workshop, ISC, and security update emails. The study conducted by Bauer et al. (2017) evaluated the effectiveness of SETA on a general user population. The present research evaluated multimodal SETA on UXAs.

Albrechtsen and Hovden (2010) developed and tested IS workshops where security personnel acted as facilitators for end-users to discuss relevant security scenarios. This small group atmosphere led to collaborative, two-way dialogs and fostered participation and collective reflection to gain insights from one another (Albrechtsen & Hovden, 2010). Safa et al. (2016) found that knowledge sharing, collaboration, intervention, experience, commitment, and personal norms were all correlated to attitude toward compliance with ISP. Sedighi et al. (2016) found reputation, reciprocity, altruism, and knowledge CA-SE were all positively related to quantity and quality of knowledge sharing while effort and time were negatively related to both. Each of these studies demonstrated the need not only to develop customized SETA aimed at improving awareness but also to build relationships amongst participants and the organization (Albrechtsen & Hovden, 2011; Safa et al., 2016; Sedighi et al., 2016).

Organizations spend significant capital on SETA programs in the hopes of increasing employee ISP compliance and engagement, but employees continue to cause significant security breaches due to their failure to comply with ISP (Yoo et al., 2018). Managers need to understand what psychological antecedents may improve the effectiveness of SETA programs and increase employee compliance (Yoo et al., 2018). Yoo et al. (2018) sought to identify the factors that influence psychological flow and how they impact SETA effectiveness and ultimately ISP compliance behavior. The

components of flow (feedback, immersion, challenge, autonomy, and social interaction) all significantly influenced psychological ownership and SETA effectiveness (Yoo et al., 2018). An important detail found by Yoo et al. (2018) was that training must be at an appropriate level to challenge but not overwhelm the participant to support engagement. Psychological ownership and SETA effectiveness significantly influenced security behavioral intention (Yoo et al., 2018). Yoo et al. (2018) suggested using relatable scenarios to help in connecting employees to the SETA content. Yoo et al. (2018) brought the concept of flow into the knowledge management realm in terms of the impact that flow has on SETA. The present research integrated relevant, real-world information into the workshop, ISC, and security update emails to assess the impact on UXA compliance behavior.

Dang-Pham et al. (2017) noted that employee IS failures could lead to security breaches causing substantial financial loss for organizations. SETA programs are effective in reducing the cost of breaches but cannot eliminate the problem of employees not following ISP due to negligence or malicious intent (Dang-Pham et al., 2017). Developing a security knowledge sharing culture may help employees gain the IS knowledge, develop an informal knowledge sharing network, and further reduce breaches caused by human error (Dang-Pham et al., 2017). Encouraging regular interactions between employees is important as some ISKS occurs during those informal dialogs (Dang-Pham et al., 2017). Also, developing trusting relationships with individuals increased formal and informal sharing between employees (Dang-Pham et al., 2017). Educating users regarding the benefits of ISP compliance, rather than just how to comply with the policy, was more effective in supporting CA-SE and inter-employee sharing

(Dang-Pham et al., 2017).

Ifinedo (2014) also studied ISP compliance and found that socialization, personal norms, social norms, CA-SE, and group dynamics positively influenced ISP compliance intention (Ifinedo, 2014). These results suggest that managers should encourage both formal and informal socialization of employees to increase trust and establish relationships that influence positive behaviors and discourage negative or malicious behaviors (Ifinedo, 2014). Developing a better understanding of the organizational and social factors that influence ISP compliance allows organizations to prepare for and encourage appropriate behavior to safeguard security. By adequately managing the IS knowledge and social norms of the organization managers can better control the antecedents of positive behavior while applying social pressure to curtail negative behavior.

Chen et al. (2018) developed a model of ISP compliance based on an Awareness-Motivation-Capacity perspective. The significant influencers of ISP compliance intention included IS awareness (awareness of the ISP and potential threats), capability to comply (CA-SE and controllability), and motivation to comply (penalty and reward) (Chen et al., 2018). Educating employees about the importance of IS can be achieved through SETA programs (Chen et al., 2018; Dang-Pham et al., 2017). These same programs can also inform employees about the organizational ISP and introduce them to the potential security threats facing the organization (Chen et al., 2018).

Development of interpersonal relationships and social networks are significant contributors to knowledge sharing within an organization (Oparaocha, 2016). SETA programs and communities of practice can help in both formal and informal sharing of

knowledge, the development of collaborative relationships, and the building of trust (Dang-Pham et al., 2017; Oparaocha, 2016). Supportive social networks can also improve relationships and encourage fostering of both cognitive-based and affective-based trust (Dey & Mukhopadhyay, 2018; Rutten et al., 2016). Trust is key for knowledge sharing relationships and the development of those relationships through an effective SETA program can be beneficial to the organization and encourage IS engagement and compliance (Dang-Pham et al., 2016; Safa & Von Solms, 2016).

The benefits of developing SETA programs that are tailored specifically to the audience were demonstrated to improve both security awareness and ISP compliance (Bauer et al., 2017; Chen et al., 2018; Ki-Aries & Faily, 2017). Bauer et al. (2017) emphasized the effectiveness of multiple training modalities on the success of SETA. The present research focused on a UXA oriented SETA workshop, ISC, and security update emails to evaluate their effectiveness in improving UXA ISP compliance behavior.

Cognitive Heuristics and Biases

Kahneman (2011) referred to the two cognitive systems of decision making as System One and System Two. System One is the intuitive, implicit, involuntary, and nonverbal cognitive system (Kahneman, 2003). According to Kahneman (2003), intuitive judgments may harken to evolutionary history and occur “between the automatic operations of perception and the deliberate operations of reasoning” (p. 697). The intuitions provided by System One come to mind quickly with little reflection—they are automatic once a stimulus occurs (West et al., 2012). Intuitions, which rely on similarity and accessibility rather than true logic or probabilities, can be flawed due to the use of cognitive heuristics (Kahneman, 2011; Tversky & Kahneman, 1974). Heuristics are

mental short cuts used to make inferences about situations, and they require a minimal amount of cognitive processing power (Gilovich & Griffin, 2013; Marsh et al., 2004; Roberts, 2004). As opposed to cognitively taxing, analytic means of solving a problem, heuristics, by their nature, do not guarantee a correct answer (Gilovich & Griffin, 2013; Roberts, 2004). Heuristics provide a means of finding an adequate solution to a problem without having to consider all possible causally relevant information (Marsh et al., 2004). Heuristics, however, help to reduce constrained working memory (Kahneman, 2011; Toplak et al., 2011). Examples of heuristics that influence decision making include anchoring, availability, illusion of pattern, subjective confidence, the law of small numbers, prediction by representativeness, and the illusion of understanding (Kahneman, 2011).

System Two, the reasoning and analytical system, is where deliberate thought occurs (Kahneman, 2011). System Two is activated whenever a problem presents itself to which System One cannot provide a fast and reasonable answer (Kahneman, 2011). Unfortunately, System One frequently will answer a difficult or challenging question with an associated question (heuristic) that is easier to draw from memory (Kahneman, 2003). Attribute substitution can allow System One to answer a question that was not asked resulting in faulty decision making (Gilovich & Griffin, 2013). One of System Two's responsibilities is to monitor System One to ensure correct decisions are made (Kahneman, 2003). To reduce cognitive load, however, System Two may accept faulty System One responses due to what Kahneman (2011) terms lazy monitoring. If System Two is engaged it may reject potentially biased System One intuitions, but that activation is cognitively taxing (Kahneman, 2003). Importantly, Kahneman (2003) found that

individuals made aware of their use of heuristics were able to correct their intuitive judgments. Education and practice can improve the reliability of System One's intuitions (Kahneman, 2003). An example of learned intuition can be found in chess masters who can quickly evaluate a chess board, analyze possible outcomes, and make moves seemingly instantaneously (Kahneman, 2003). Kahneman (2003) demonstrated that training improved intuition. This demonstrated the potential for improving the intuitive responses of UXA through an effective and engaging SETA workshop and ISC.

Epstein (2014), in the field of cognitive psychology, defined the two cognitive systems as the experiential system and the rational system. The experiential system functions outside of an individual's awareness and influences interpretation of feelings, behaviors, and events (Epstein, 2014). The experiential system is non-verbal, and activation requires minimal cognitive demand (Epstein, 2014). A key feature of the experiential system relevant to the current research is that it has the potential to learn from experience (Epstein, 2014). The rational system reflects an individual's personal understanding of logic and is uniquely human (Epstein, 2014). It represents conscious reasoning, verbal thought, tends to be affect free, considers cause and effect, is slower processing, and requires higher cognitive load (Epstein, 2014).

Toplak et al. (2011) analyzed the use of the Cognitive Reflection Test (CRT) to assess cognitive performance. They found that the CRT predicted an individual's propensity toward cognitive errors (Toplak et al., 2011). Toplak et al. (2011) studied intelligence and working memory and found both were moderately predictive of rational thinking skills and cognitive performance. The conclusion was that the quick acceptance of the System One data was primarily due to cognitive load and the miserly cognitive

processing of System Two (Toplak et al., 2011). These findings are in line with Kahneman's (2011) lazy monitoring performed by System Two. Toplak et al. (2011) warned that while the intuitive processing of System One may be useful it can also be dangerous due to the propensity to oversimplify problems and underestimate risk.

Ferreira et al. (2006) investigated heuristic problem-solving skills to understand what actions might encourage System Two engagement. Using modified versions of Tversky and Kahneman's (1974) heuristic problem set, Ferreira et al. (2006) found that providing priming instructions to participants helped them to resist System One intuitions and engage System Two reasoning. Kliger and Kudryavtsev (2010) defined priming as an unconscious process that occurs when a current stimulus increases the availability (recall) of past associations. Increased use of System Two resulted in significantly improved performance on the heuristic problems (Ferreira et al., 2006).

OB can result in dangerous neglect of risks (Pfleege & Caputo, 2012; Rhee et al., 2012). OB leads one to assess situations in self-serving ways (Rhee et al., 2012). This fundamental underestimate of risk can enhance perceived invulnerability to negative events and lead to inappropriately low levels of safeguarding behaviors related to IS (Rhee et al., 2012). OB is a protective measure to protect the self, and reduce both anxiety and stress (Rhee et al., 2012). In a study of IS perceptions of technology executives, Rhee et al. (2012) found that they perceived security risks, but that OB allowed them to conclude that their organizations were at a much lower risk of security breach than other organizations. Rhee et al. (2012) suggested IS training is key to reducing OB and improving security practices within organizations. OB can also cause individuals to discount future consequences (Kahneman, 2011; Rhee et al., 2012). For

example, one may believe they are not at risk of intrusion and therefore not adequately protect personal privacy (Acquisti, 2004). In the present research, OB was studied to evaluate if it could be blinding UXAs to the true threats facing their servers. Pfleeger and Caputo (2012) suggested OB reduces ISP compliance behavior but can be minimized by making SETA personally relevant to the learner.

CB and OB are closely related and can significantly influence decision making (Kahneman, 2011). With CB, one gives greater validity to information that supports rather than contradicts one's beliefs (Pfleeger & Caputo, 2012; Sternberg, 2004). Tsohou et al. (2015) found that CB may lead individuals to believe that hackers are not sophisticated or inappropriately assess the security threats caused by nation states and organized crime. Kahneman (2011) identified CB as a System One heuristic and it is therefore easily activated when making decisions. System Two must be engaged to override CB but in most situations, individuals do not devote the cognitive energy to disprove their strongly held beliefs (Kahneman, 2011). The exaggeration of events in the news can reinforce CB and result in faulty assumption of risks-discounting risks with higher probabilities over risks that are more easily recalled (Kahneman, 2011). The prevalence of news related to Windows server breaches and vulnerabilities may erroneously confirm for the UXAs that their servers are not at risk and they may discount any evidence to the contrary. Pfleeger and Caputo (2012) suggested that providing "an arsenal of evidence" may be necessary to counter confirmation biased thinking (p. 606).

To judge the frequency or probability of an event an individual may assess the availability of associations related to the event (Pfleeger & Caputo, 2012; Tversky & Kahneman, 1974). Rather than taking the time to consider an actual probability it is easier

to estimate a probability based on the ease that one recalls occurrences of a similar event, termed the AH (Kahneman, 2011; Kliger & Kudryavtsev, 2010; Tversky & Kahneman, 1974). In assessing how the AH influenced individual's judgment of risks, Pachur et al. (2012) found that the AH significantly influenced perceived risk. Since a question about frequency is difficult to answer, an easier question is substituted (i.e., how easily can examples of the event be recalled) (Kahneman, 2011). If examples come to mind easily, the frequency is estimated to be high and if examples are difficult to imagine the frequency is assumed to be low (Tversky & Kahneman, 1974). System One does not typically have the means to properly apply probability theory and the reliance on availability as an assessment of actual probability can lead individuals to faulty evaluations of risk (Kahneman, 2011). If UXAs employed the AH they may be incorrectly assessing a lower security risk to their servers because they more easily recall data breaches, security alerts, or reported fixes associated with Windows servers. Without a correct assessment of potential risks, the UXAs may not have perceived the true threat severity or threat vulnerabilities to their servers. This bias can potentially result in insufficiently secured servers, leaving them at higher risk of breach. Pfleeger and Caputo (2012) suggested that developing SETA that is vivid and provides personally relatable examples of breaches may improve ISP compliance behavior.

Kahneman's (2011) work has had significant influence on the finance industry in researching investment decisions, but using his concepts in the IS area, has been limited. Heuristics and biases associated with the dual-process theory are applicable to the IS realm given that they may influence UXAs decisions. System One's automatic and intuitive assessments can be prone to error (Kahneman, 2011). Associative processing

System One tends to best-guess answers to questions with available data even when that data is not completely relevant to the posed question (Pennycook et al., 2013; West et al., 2012). Kahneman (2011) referred to this as the shotgun effect. Another potential area of concern is the way that System One deals with ambiguities and competitive hypotheses eliminating options before cognitive awareness (Kahneman, 2003). When System Two is not actively monitoring System One, to assess the validity of the decisions, errors may occur (Kahneman, 2011; Toplak et al., 2011). Building on Kahneman's (2011) heuristics and biases work in assessing risk, this study investigated how cognitive heuristics and biases influenced UXAs decisions regarding security threat appraisal, coping appraisal, CA-SE, and CA-RE. Security risks and threat vectors in IS continue to evolve (Caballero, 2013). It is crucial to have competent and engaged UXAs that acknowledge the security threats and work diligently to mitigate the risks to their servers (Caballero, 2013).

Based on the prior research noted above, simple unconscious acceptance of System One responses may cause UXAs to underestimate risks and vulnerabilities facing their servers. By better understanding what heuristics impact how decisions are made, what biases may result, and learning how to encourage System Two processing, organizations may be better prepared to manage their administrators and reduce security risks (Kahneman, 2011; Pennycook et al., 2013; West et al., 2012).

Protection Motivation Theory

PMT is frequently used to understand compliance with ISPs and security procedures (Hanus & Wu, 2016; Safa et al., 2015; Siponen et al., 2014). PMT was initially proposed by Rogers (1975) to help understand how health behaviors were influenced by fear appeals. Rogers (1975) theorized that relevant sources of information

that influenced behavioral change include environmental data (verbal persuasion and observational learning) and intrapersonal data (personality and prior experience). These sources are evaluated through a cognitive mediation process that assesses the threat and coping potential which leads to adaptive or maladaptive coping behaviors (Rogers & Prentice-Dunn, 1997). Threat appraisal includes the positive factors of extrinsic and intrinsic rewards offset by negative factors of the TA-PS and TA-PV to potential threats (Posey et al., 2015; Rogers & Prentice-Dunn, 1997; Vance et al., 2012). Coping appraisal is an assessment of how the individual can cope with, adapt to, and change behavior to avoid the danger (Rogers & Prentice-Dunn, 1997; Vance et al., 2012). The factors related to coping appraisal include an individual's CA-SE and CA-RE (Posey et al., 2015). CA-RE is an evaluation of the effectiveness of the proposed behavior to reduce the probability of the negative event (Rogers & Prentice-Dunn, 1997; Vance et al., 2012). CA-SE is the belief that one is capable of the adaptation necessary to mitigate the negative event (Rogers & Prentice-Dunn, 1997). TA-PS is an evaluation of the potential physical, psychological, social, or economic harm an individual expects may occur (Rogers & Prentice-Dunn, 1997). TA-PV is an assessment of probability a negative event will occur if no changes are made to the individual's behavior (Rogers & Prentice-Dunn, 1997; Vance et al., 2012). Fear influences the evaluation of severity and vulnerability and indirectly influences behavioral intention (Rogers & Prentice-Dunn, 1997). Siponen et al. (2014) found TA-PS of threat and TA-PV to be positively correlated with ISP compliance intention. Appropriate threat appraisal can be manifest through increased knowledge and awareness of IS risks, vulnerabilities, and organizational policies and procedures (Albrechtsen & Hovden, 2010; Guo et al., 2011; Safa & Von Solms, 2016; Siponen et al.,

2014). Coping appraisal can be also be positively influenced by ISKS and awareness (Safa et al., 2015; Siponen et al., 2010). Rogers and Prentice-Dunn (1997) noted that there are numerous cognitive heuristics and biases that can influence both appraisal processes in the PMT model. Cognitive heuristics can lead to cognitive biases and influence daily decision-making without our awareness (Kahneman, 2011). As such, it is important to understand how heuristics and biases influenced the threat appraisal of UXA and design awareness and training programs that encourage System Two processing. If threats are perceived as “Windows problems” the precognitive choice to resist ISP implementation on UNIX servers may put the organization at considerable risk.

In a study of home computer users, Hanus and Wu (2016) evaluated how awareness, a potential antecedent of desktop security behavior, influenced user’s security actions. Hanus and Wu (2016) extended PMT by defining the multi-dimensional construct of awareness (threat awareness and countermeasure awareness) to understand how awareness may influence desktop security behaviors. The goal of this study was to determine if threat awareness and countermeasure awareness, as antecedents of PMT, influence desktop security behavior (Hanus & Wu, 2016). Hanus and Wu (2016) demonstrated that research into the antecedents of PMT can provide a clearer picture into security behavior. Hanus and Wu (2016) identified both threat awareness and countermeasure awareness as key points for training to improve desktop security behavior. Hanus and Wu (2016) acknowledged that there may be a hidden variable that influences the relationship between threat awareness and TA-PV that has not been discovered through existing research. Hanus and Wu (2016) demonstrated how PMT can be extended by including awareness. Awareness can be facilitated through effective

training and knowledge management within an organization (Bauer et al., 2017; Dang-Pham et al., 2017).

Bélanger et al. (2017) in a study of early adopter password compliance, found that perceived threat severity and perceived threat vulnerability were positively related to attitude toward ISP change. Organizational triggers and ISP awareness had a positive correlation with attitude and intention to comply (Bélanger et al., 2017). Interestingly, Bélanger et al. (2017) found that subjective norm and CA-SE did not significantly influence intention to conform to ISP for early adopters. The inclusion of perceived threat severity and perceived threat vulnerability from PMT was crucial to understanding the antecedents to attitude and intention (Bélanger et al., 2017).

Posey et al. (2015), investigated the impact of SETA programs on PMT. Specifically, Posey et al. (2015), evaluated constructs frequently unused when applying PMT to IS contexts, including response costs, intrinsic and extrinsic maladaptive behaviors, and fear. The goal of the research by Posey et al. (2015) was to fully test PMT in an IS context adding SETA as an antecedent and organizational commitment as a moderating variable to better understand IS behavior. SETA was positively correlated with both perceived threat severity and perceived CA-RE indicating that SETA programs are an effective way of encouraging IS behavior (Posey et al., 2015). Appropriately designed SETA programs can help reduce the human IS risk to organizational assets (Van Vuuren, 2016; Whitman & Mattord, 2012).

Safa et al. (2015) conducted research to identify the factors that influence user's IS conscious behavior with antecedent factors of IS awareness, organizational policy, experience, and involvement. Security conscious behavior by users can help to mitigate

IS risk (Safa et al., 2015). The study found that by increasing a user's awareness of risks and vulnerabilities, improvements in attitude and IS conscious behavior can be achieved (Safa et al., 2015). Additionally, engaging users in the process of securing their systems, and educating them regarding potential threats improves threat appraisal and CA-SE and positively influences IS conscious behavior (Safa et al., 2015). Knowledge sharing and collaboration are key components of this model in terms of IS awareness, organizational policy (and communication), involvement, engagement, and behavior (Safa et al., 2015). Vance et al. (2012) suggested that developing SETA programs that make participants aware of cybersecurity threats, the importance of ISP compliance, and the role that employees play in maintaining the security and integrity of organizational data will help to improve proper threat appraisal, coping appraisal, CA-SE, and CA-RE. Accordingly, the present research developed a SETA workshop, an ISC, and six security update emails that make UXAs aware of threats and risks to encourage proper evaluation of CA-SE and threat appraisal.

One of the challenges in ISP compliance studies that use PMT noted by Boss et al. (2015) is the focus on intention rather than actual behavior. Boss et al. (2015) found few studies had been conducted that evaluated actual secure behaviors (Boss et al., 2015). Intention frequently differed from actual implementation of security controls (Boss et al., 2015). Boss et al. (2015) conducted four field experiments to evaluate PMT in the context of IS and found that the strength of the fear appeal significantly influenced compliance intention and behavior. The present research used security scans and other tools to verify actual security measures implemented by the UXAs to evaluate compliance.

Information Security Policy Compliance

Although organizations spend considerable money on IS technology, users are still a major source of failures that result in IS breaches costing organizations substantial financial loss (Safa et al., 2016). ISPs elucidate the required security processes employees must follow to ensure the confidentiality, integrity, and availability of organizational IT resources (D'Arcy & Lowry, 2019; Van Vuuren, 2016). ISPs include formalized procedures, guidelines, and technical controls that employees must follow to meet organizational security requirements (Cram et al., 2017; Lowry & Moody, 2015). The human aspects of IS must be understood to reduce the risk of IS breaches (Van Vuuren, 2016). Users' ignorance, apathy, resistance, or mischievous nature may result in human error and allow IS breaches to occur (Bélanger et al., 2017; Safa et al., 2016).

Compliance with ISP can help to mitigate IS risk (Ifinedo, 2014). Employee noncompliance with ISP remains as a threat to organizational IS (Siponen et al., 2014). Given the critical nature of organizational data and the significance of human behavior in protecting data, developing an understanding of what factors encourage and discourage ISP compliance may help to protect organizations (Bélanger et al., 2017; Carlton & Levy, 2015; Van Vuuren, 2016).

Researchers have developed many theoretical models to understand ISP compliance. Siponen et al. (2014) combined PMT, the Theory of Reasoned Action (TRA), and Cognitive Evaluation Theory (CET) to develop an integrated theory that better explains end user ISP compliance intention. They found that awareness of security vulnerabilities and risks improved ISP compliance intention (Siponen et al., 2014). Compliance intention, however, has not been found to consistently indicate AC behavior

in the IS context (Blythe et al., 2015; Crossler et al., 2013).

Safa et al. (2016) sought to identify the factors that influence ISP attitude toward compliance and found that ISKS, collaboration, intervention, commitment, and personal norms all significantly influenced attitude toward compliance and behavioral intention (Safa et al., 2016). Like Siponen et al. (2014), a key limitation of the study conducted by Safa et al. (2016) was that they only evaluated behavioral intention not actual IS compliance behavior.

Many studies have assessed ISP compliance intention using surveys (Dang-Pham et al., 2017; Ifinedo, 2014; Safa et al., 2016; Yoo et al. 2018). Using this method to assess actual ISP compliance behavior is suspect due to the potential for social desirability biased self-reporting (Crossler et al., 2013; Redmiles et al., 2017). Crossler et al. (2013) suggested several potential techniques to minimize this risk including scenarios, hypothetical situations, longitudinal studies, and field experiments. Assessing compliance intention using a subjective, self-reported survey, while easier for the researcher, does not afford a true assessment of compliance behavior (Blythe et al., 2015). An objective measure of compliance is more challenging but can afford a better understanding of actual ISP compliance (Blythe et al., 2015). Given these risks, it is preferred to study actual IS behavior rather than relying on self-reported intention to comply to develop valid and reliable behavioral models (Crossler et al., 2013). The present study operationalized the UXA's actual security compliance behavior via quantifiable measures that were determined via Tenable Nessus dashboard data, Splunk data, or programmatically via script.

Vulnerability scans and penetration testing are effective means of identifying

server vulnerabilities (Fashoto et al., 2018; Haber & Hibbert, 2018). Vulnerability scans can identify weaknesses in systems and applications so that systems administrators can eliminate or mitigate them thereby reducing risk of breaches (Fashoto et al., 2018; Samtani et al., 2016). The types of information gathered by scans include errors in design, implementation, coding, or configuration that can be exploited by threat actors (Haber & Hibbert, 2018). Passive scans can be used to listen to network traffic and intuit conclusions about systems actively communicating on the network (Haber & Hibbert, 2018). These external scans, however, are limited in the amount of data they can collect about servers and can provide erroneous results (Brotherston & Berlin, 2017; Tenable, 2019). Active scans can be credentialed or uncredentialed and actively access the target to assess potential vulnerabilities (Asadoorian, 2010; Helms et al., 2017; Jetty & Rahalkar, 2019; Meyers & Jernigan, 2018). Uncredentialed scans mimic what attackers may see as exploitable vulnerabilities, but they identify significantly less of an asset's true vulnerabilities (Brotherston & Berlin, 2018; Haber & Hibbert, 2018). A credentialed vulnerability scan uses valid user credentials to authenticate to a server and preform commands to gather detailed information about the server (Asadoorian, 2010; Brotherston & Berlin, 2017; Helms et al., 2017). Credentialed scans allow for detailed server and application patch analysis, as well as a thorough evaluation of user, password, and directory settings (Asadoorian, 2010). Credentialed scans can also assess configuration settings, identify local software exposures, detect malware, and perform database testing (Meyers & Jernigan, 2018; Tenable, 2019). In a study comparing credentialed and uncredentialed scans Fashoto et al. (2018) found credentialed scans found 634 vulnerabilities while the uncredentialed scans found only 163. Credentialed

scans provide a more complete picture of the vulnerabilities and the attack surface of the target servers (Jetty & Rahalkar, 2019). Additionally, credentialed scans can perform more tests and provide more accurate results (Tenable, 2019). Haber and Hibbert (2018) suggested that vulnerability scanning should be performed on all servers within an organization due to the risk an attacker can breach one server and move laterally throughout an enterprise's network.

Tenable Nessus is one of the most popular enterprise vulnerability assessment tools available (Helms et al., 2017; Jetty & Rahalkar, 2019; Meyers & Jernigan, 2018; Samtani et al., 2016). Nessus can perform safe scans, intrusive scans, policy compliance tests, detailed patch audits, client-side software vulnerability testing, service discovery, port discovery, password checking, database authentication testing, and provide remediation information (Asadoorian, 2010; Tenable, 2019). Nessus has 80,000+ plugins, written in Nessus Attack Scripting Language, that can analyze server configurations and identify vulnerabilities (Jetty & Rahalkar, 2019; Samtani et al., 2016). Each plugin contains information on the specific vulnerability, remediation actions, and an algorithm for testing for the vulnerability (Tenable, 2019).

Nessus can classify vulnerabilities using the Common Vulnerability Scoring System (CVSS), which includes a base score, temporal metric, and exploitability metric (Haber & Hibbert, 2018; Tenable, 2019). CVSS is a common severity rating system for classifying IS threats (Brotherston & Berlin, 2017). The CVSS base score includes ratings of vulnerabilities based on access complexity, access vector, privileges required, and authentication method (Haber & Hibbert, 2018). CVSS temporal metrics include the complexity of the exploit, remediation level, and confidence (Jetty & Rahalkar, 2019).

The CVSS exploitability metric indicates the maturity of the vulnerability and indicates if it is unproven, proof of concept, functional, or high (Haber & Hibbert, 2018; Jetty & Rahalkar, 2019). The resulting CVSS rating is a score from one to 10 indicating the risk the vulnerability presents (Haber & Hibbert, 2018; Jetty & Rahalkar, 2019). Quantitative CVSS scores can be translated into standardized qualitative severity ratings (First.org, n.d.). A CVSS score from 0.1 to 3.9 represents a low severity rating, from 4.0 to 6.9 represents a medium, 7.0 to 8.9 represents a high, and 9.0-10.0 is critical (First.org, n.d.).

By performing credentialed vulnerability assessments, Tenable Nessus can identify the security vulnerabilities on target servers (Tenable, 2019). Creating a baseline assessment of a server can help to delineate server and configuration changes made by administrators between the successive scans (Jetty & Rahalkar, 2019). In the present study, Tenable scans, Splunk scans, and scripts were run prior to the SETA workshop, ISC, and security update emails to establish a baseline on key elements that were presented during the training. Three months following completion of the workshop, ISC, and security update emails another round of scanning was run to assess actual security changes implemented on participant's servers.

Summary

Based on a review of the literature, there are several notable gaps that this study investigated. First, research on ISP compliance has focused primarily on end-user compliance intention (Albrechtsen & Hovden, 2010; Dang-Pham et al., 2017; Hanus & Wu, 2016; Ifinedo, 2012; Safa et al., 2016). It was crucial, however, to understand the determinants of server administrator ISP compliance behavior to better ensure the confidentiality, integrity, and availability of PII and PHI data contained on their servers.

Second, this study focused on formal knowledge sharing arrangements from the security knowledge-sharing framework developed by Flores et al. (2014). Specifically, this research investigated how a SETA workshop, designed specifically for UXAs, affects ISKS, use of heuristics and biases, and ISP compliance behavior. Concentrating on this specific user group for education was unique and helped to evaluate the effectiveness of a workshop that encouraged collaboration, knowledge sharing, and use of UXAs related scenarios. Third, cognitive heuristics can lead to biased decision making and biased evaluation of IS threats and risks (Kahneman, 2011; Pachur et al., 2012; Rhee et al., 2012; Toplak et al., 2011; Tsohou et al., 2015). The inappropriate use of heuristics may prevent UXAs from correctly assessing the risks to their servers, which may reduce ISP compliance behavior. SETA programs can be an effective means of reducing bias and improving security behaviors (Rhee et al., 2012; Wash & Cooper, 2018). It was crucial to learn how to reduce the use of cognitive heuristics to minimize biased decisions. Fourth, PMT has been established as an effective model for evaluating ISP compliance intention and behavior (Boss et al., 2015; Johnston et al., 2015). SETA programs have positively influenced threat appraisal and coping appraisal (Posey et al., 2015). They have also been established as precursors of compliance intention and behavior (Boss et al., 2015; Siponen et al., 2014). While Posey et al. (2015) integrated SETA and PMT, their focus was limited to end-user behavioral intention. Also, Posey et al. (2015) did not include the influences of heuristics, and biases on SETA effectiveness. Finally, while behavioral intention is frequently taken as an indicator of behavior, it was noted by Crossler et al. (2013), that actual behavior may not follow reported intention due to biased self-reporting. Boss et al. (2015) also found that intention differed significantly from actual

implementation of security controls. Comparing baseline and post-intervention security scans allowed the present research to analyze security measures implemented by UXA and this afforded unique insights into the effectiveness of the training in terms of actual implementation of security controls and ultimately ISP compliance behavior. This research was needed as implementing mandated security and compliance with organization ISP is key to the successful protection of healthcare organizational assets, including patient PHI and PII (Koch, 2017; Ng et al., 2009).

Chapter 3

Methodology

Overview

This chapter presents the research design, instrument development, approach, population, sampling, data collection, and data analysis used to assess the influence of the SETA workshop, ISC, and security update emails on UXAs use of cognitive heuristics, biases, and ultimately ISP compliance behavior. Additionally, reliability and validity of the instrument was addressed.

Research Design

This quantitative research was conducted in a pretest and posttest design. Participants completed the survey (Appendix A) prior to and following the intervention (Sekaran & Bougie, 2013). They participated in the new SETA workshop and an ISC (Appendix B). Bauer et al. (2017), in a study of ISP compliance at banks, found that developing a comprehensive, multi-modal IS awareness program was key to successfully establishing an IS culture in an organization. Caballero (2013) also found that combining multiple formats for SETA (i.e. computer-based training, simulators, phishing email campaigns, face-to-face training) into highly customized, job specific job programs was key to increasing secure behaviors.

The SETA workshop focused on increasing awareness of cyber risks, vulnerabilities, and presented specific security recommendations for UXAs servers (Beuchelt, 2017a; Inshanally, 2018; US Department of Health and Human Services, 2013). The organizational Information Security and Risk Management Plan (ISRMP) was

used to prioritize the top 12 security strategies that were relevant to server administration. This document prioritized IS risk based on the likelihood, risk, and potential organizational impact. Specifically, the ISRMP identified the following critical server management areas: patch management (operating system, microcode, and third-party apps), vulnerability analysis (extensive Tenable and Accunetix scanning), privileged account and access management (password requirements and multifactor authentication), centralized log management (Splunk), and developing administrator's digital forensics skills.

The SETA workshop was conducted online via a secure Zoom meeting and included IS team members, and UXA within the organization. A total of 50 UXA from multiple departments participated. Six additional individuals participated including the CISO, the director of Engineering Services, as well as several network security team members and two database administrators. The workshop encouraged connection, collaboration, discussion, and ISKS between the participants (Albrechtsen & Hovden, 2010). The overarching goal of this workshop was to improve UXA ISP compliance behavior. This was accomplished by increasing participant awareness of the current state of cyber-attacks, the costs associated with data breaches, the growing list of software vulnerabilities, types and motivations of perpetrators, and how to best mitigate cyber vulnerabilities for their servers. The security workshop introduced UXA to available reports and online resources that they can use to increase and maintain their awareness of the current state of cyber threats, risks, and vulnerabilities. The workshop demonstrated the need for constant monitoring of vulnerabilities and ultimately the vital need to secure UNIX servers to mitigate risk and prevent loss. Additionally, participants were introduced

to several penetration testing tools including nmap, Wireshark, and the Metasploit Framework. By learning to utilize tools used by penetration testers, the workshop and ISC provided UXAs additional resources that can be used to test and secure their servers effectively which may increase ISP compliance behavior. The material for the workshop was reviewed by the organization's CISO for content. Modifications to the content were made based on the feedback from the CISO to further align the material with the cybersecurity goals of the organization and tailor the material to the unique role of UXAs.

The learning objectives for the SETA workshop were: By the end of this workshop, the participants will:

- 1) Help maintain by:
 - a. Discussing the scope and impact of data breaches,
 - b. Learning about key websites that provide critical and timely information about software and hardware vulnerabilities,
 - i. Verizon Data Breach Investigations Report (Verizon, 2019),
 - ii. Privacy Rights Clearinghouse (n.d.),
 - iii. U.S. Department of Health and Human Services Office for Civil Rights Breach Portal,
 - iv. National Vulnerability Database.
 - c. Identifying different types of cyber attackers and their motivations,
 - d. Learning about cyber-attacks made against our organization,
 - e. Discussing the cost of a HIPAA breach,
 - f. Discussing our implementation of Defense in Depth
 - i. Firewalls/Intrusion prevention systems (IPS),

- ii. Security Event/Information Management (SIEM),
- iii. Identity and rights management,
- iv. Anti-phishing campaigns,
- v. Advanced endpoint protection,
- vi. Threat intelligence,
- vii. Behavioral analytics,
- viii. Penetration testing,
- ix. Cyber forensics.

2) Help participants mitigate security risk for their servers by:

- a. Reviewing the phases of cyber-attacks and threats typically used to exploit servers,
 - i. Reconnaissance,
 - ii. Intrusion,
 - iii. Exploitation,
 - iv. Escalate privilege,
 - v. Lateral movement,
 - vi. Anti-forensics,
 - vii. Denial of service,
 - viii. Data exfiltration.
- b. Discussing the types of cyber attackers
 - i. Cyber criminals – identity theft and financial fraud with goal of monetary gain,
 - ii. Script kiddies – minimal skills, use available exploit kits,

- iii. Brokers – uncover vulnerabilities in software or systems and sell the information,
 - iv. Insiders – employees, partners, and contractors motivated by perceived wrong,
 - v. Competitors – individuals and organizations seeking to gain competitive advantage,
 - vi. Cyberterrorists – disable and disrupt network or computing infrastructure,
 - vii. Organized crime – highly funded, high-level of skill, seek financial gain,
 - viii. Hacktivists – political, social, or principle-based agenda,
 - ix. State-sponsored attackers / nation state – highly funded and skilled, intelligence gathering or service disruption, focus is government interests.
- c. Identifying the top threats and risks facing our organization's servers,
- i. Key threats and vulnerabilities
 - 1. Compromised credentials and privilege escalation,
 - 2. Web service exploitation,
 - 3. Server vulnerabilities that permit remote code execution,
 - 4. Cryptography weaknesses,
 - 5. Deserialization,
 - 6. Scripting,
 - 7. Malware, fileless malware, and rootkits.

- ii. Key exploits facing servers
 - 1. Buffer and stack overflows,
 - 2. Memory corruption,
 - 3. Race conditions,
 - 4. SQL injection.
- d. Identifying 12 activities, settings, and tools participants can use to improve the safety and security of their servers,
 - i. Minimize services / disable unwanted services / limit open ports to reduce vulnerabilities and attack vectors,
 - ii. Remove unnecessary software to reduce the number of vulnerabilities and potential attack vectors,
 - iii. Keep Linux/UNIX kernel and other software as up to date as possible,
 - iv. Ensure strong password policies and account management,
 - v. Kernel hardening to protect against attacks,
 - vi. Configure the server's local firewall,
 - vii. Disk security – file integrity checking, file system encryption,
 - viii. Configure SSH security settings,
 - ix. Implement Security Enhanced Linux,
 - x. Configure centralized log management,
 - xi. Perform monthly vulnerability scans on servers,
 - xii. Run Malware detection software to detect worms, viruses, and rootkits.

- e. Learning about available enterprise tools and other locally administered tools participants can use for vulnerability analysis and security monitoring.
- 3) See how to perform basic penetration testing and server analysis using common tools by:
- a. Using nmap for enumeration, scanning, and vulnerability analysis on servers,
 - i. Ping scan,
 - ii. Version scan,
 - iii. Vulnerability scan.
 - b. Using Wireshark for network traffic analysis for security monitoring and problem resolution,
 - i. Search and filter options,
 - ii. Protocol inspection,
 - iii. Live network traffic capture,
 - iv. Offline network traffic analysis
 - c. Using the Metasploit Framework in action and its utility to identify, enumerate, and exploit a server
 - i. Reconnaissance & Scanning/Enumeration,
 - ii. Exploitation demo:
 - 1. VSFTPD,
 - 2. Ssh,
 - 3. Mysql,

4. Samba.

- 4) Access a cloud-based Cyber lab to:
 - a. Get hands-on experience using nmap and the Metasploit Framework (MSF) in a secure, cloud-based virtual environment,
 - b. Identify, enumerate, breach, and exploit a Linux VM using MSF tools,
 - c. Compete to find the most flags on the Linux target machine.
- 5) Connect with other UNIX administrators to increase knowledge sharing and collaboration:
 - a. Joining a new Microsoft Team's Team for UXA in the organization.

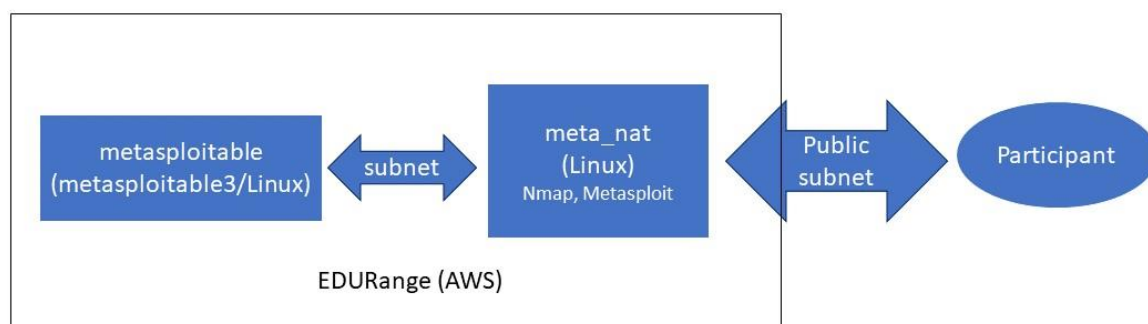
The ISC immediately followed the workshop provided hands on experience using security tools in an environment that was both remote and secure. The module utilized Linux VMs and consisted of challenges associated with locating, enumerating, and exploiting a server. EDURange (2019) provides cloud-based resources for security education of students and researchers. A new EDURange scenario was developed as part of this study and provided a secure, remote, cloud-based environment where the UXA performed penetration testing. Providing hands-on security experience has been found to increase participant engagement, improve retention, and encourage ISP compliance behavior (Bauer et al., 2017; Caballero, 2013).

For the ISC module, two Linux VMs were instantiated for every 10 participants: a participant VM (meta_nat) and a target metasploitable3 server (metasploitable) (Figure 2). The private IP addresses for these servers were 10.0.37.6, and 10.0.20.4 respectively. The public IP address, which is the gateway into the environment, varied and was defined when each scenario was instantiated. The day of the workshop participants received an

email with the login information needed to access the ISC. This included the public network address, as well as a unique user id and password. Additionally, participants received an instruction sheet (Appendix C) that provided some materials from the workshop as well as hints and tips to be successful with the ISC.

Figure 2

ISC Virtual Layout



The learning objectives for the ISC module are: By the end of the ISC, the participants will:

- 1) be able to perform network reconnaissance, server enumeration, port and service enumeration using nmap to identify a vulnerable Linux server on an isolated network,
- 2) be able to use the Metasploit framework on a Linux VM,
- 3) be able to identify a relevant exploit to use to gain command line access to a Linux server,
- 4) be able to locate, download, and hash Capture the Flag (CTF) target files.

For this module, participants scanned the network segment using nmap to perform a ping sweep and identify the target server. Participants then used a nmap version scan to identify the ports, services, and software running on the target Linux VM

(metasploitable). Next, participants used the Metasploit framework to search for and identify potential exploits for the target VM. Finally, participants exploited a vulnerability and breached the Metasploitable VM. Once participants gained access to the VM they located, downloaded, decoded, and hashed CTF target files.

Following the workshop, every three weeks, UNIX security update emails were sent to each participant (Appendix D). A total of four UNIX security update emails were sent to participants during the study. These emails provided an update regarding recently identified vulnerabilities, relevant CERT alerts, recent breach announcements, as well as an invitation to join the new Microsoft Teams group set up for collaboration. In August, two additional emails were sent to provide UXAs additional information about Tripwire and Rootkit Hunter applications. These emails included installation, configuration, and testing information to expose the UXAs to these tools that were presented during the workshop. The goals of the security update emails were to maintain current cybersecurity awareness, increase security knowledge sharing, and reinforce security recommendations made during the workshop.

Finally, three months after the workshop, an email was sent to the participants to complete the online survey. Additionally, the participants servers were reanalyzed to quantify the changes made by the UXAs during the study and evaluate the effectiveness of the workshop, ISC, and UNIX security update emails.

Instrument Development and Validation

The survey instrument was developed based on prior research and augmented with researcher-developed questions for the AH, CB, and OB. Questions for CA-SE, CA-RE, TA-PV, TA-PS, OB, and ISKS were adapted from previously validated instruments

used by Safa and Von Solms (2016), Moqbel and Bartelt (2015), Ifinedo (2012, 2014), Hanus and Wu (2016), Rhee et al. (2012), Siponen et al. (2014), and Safa et al. (2016). As a courtesy, a request was sent to each of the researcher teams asking permission to modify and use their questions in the present research. All acknowledged the request and provided their permission to modify and use their questions in the present research survey (Appendix E).

The survey was pilot tested (Appendix F) with sixteen individuals who evaluated the flow of the survey, the wording of the questions, as well as the reliability and validity of the instrument. The experts consisted of four professors with doctoral degrees, nine doctoral student researchers, and four IS field experts. The reviewers' backgrounds included the fields of IS, information systems, IT, decision science, UNIX administration, and information assurance. Participant reviewers used Qualtrics to analyze the survey and provide feedback. Based on their responses, several modifications were made. Regarding survey flow, the number of survey blocks was reduced, a progress bar was added, and the back button was removed. Regarding the CB questions, the instruction was modified, the time for responses was increased, and the format of the choices was changed. Regarding content, several questions were removed, and several questions were modified for clarity as well as consistency. Finally, one additional question was added for TA-PV. The final survey consisted of 25 questions and was administered to participants online using the Qualtrics Survey tool. Questions 1-23 used a seven-point Likert scale: strongly disagree (1), disagree (2), somewhat disagree (3), neither agree nor disagree (4), somewhat agree (5), agree (6), strongly agree (7). The selection of a seven-point Likert with a central point was based on Hair et al. (2017) suggestions that symmetric Likert scales can be

used in SEM as an approximation of an interval measurement. Table 1 provides a detailed listing of the constructs used in the research model, the indicators used in the survey, the question numbers associated to each indicator in the survey, and the sources of the survey items. The demographic question related to age was based on Super's career stages ages of exploration, establishment, mid-career, late-career, and decline (Gothard et al., 2001).

Table 1

Constructs and Sources

1st Order Construct	Indicators	Question Number	Source
CA-SE	SE1	1	Ifinedo (2014)
	SE2	2	Ifinedo (2014)
	SE3	3	Ifinedo (2014)
CA-RE	RE1	4	Ifinedo (2012)
	RE2	5	Ifinedo (2012)
	RE3	6	Ifinedo (2012)
TA-PV	PV1	7	Hanus and Wu (2016)
	PV2	8	Siponen et al. (2014)
	PV3	9	Ifinedo (2012)
	PV4	10	Based on reviewer feedback
TA-PS	PS1	11	Siponen et al. (2014)
	PS2	12	Hanus and Wu (2016)
	PS3	13	Siponen et al. (2014)
ISKS	ISKS1	14	Safa et al. (2016)
	ISKS2	15	Safa et al. (2016)
	ISKS3	16	Safa et al. (2016)
OB	OB1	17	Rhee et al. (2012)
	OB2	18	Rhee et al. (2012)
	OB3	19	Rhee et al. (2012)
AH	AH1	20	Researcher developed
	AH2	21	Researcher developed
	AH3	22	Researcher developed
	AH4	23	Researcher developed
CB	CB1	24	Researcher developed, based on Fischer et al. (2011).
Demographic	AGE	25	

In the questions derived from Ifinedo (2014), Hanus and Wu (2016), and Siponen

et al. (2014), references to “computer” were changed to “servers” to reflect the focus on UXAs servers. The AH and conformation bias questions were time-limited to encourage use of Kahneman’s (2011) System One processing and limit use of System Two’s more thorough analysis. These techniques are similar to the ones used by Finucane et al. (2000) as well as Gertner et al. (2016). Confirmatory bias was tested using a fictional scenario, like the technique of Fischer et al. (2011). Table 2 identifies the constructs of the model, the survey questions, Qualtrics survey number, and the hypotheses tested for each. The difference in the Qualtrics survey number is due to text dialogs, design flow, and timing questions which do not appear to the participant.

Table 2

<i>Constructs and Hypotheses</i>		
Construct	Survey questions	Hypothesis
CA-SE	1-3	H8a
CA-RE	4-6	H8b
TA-PV	7-10	H7b
TA-PS	11-13	H7a
ISKS	14-16	H1, H2, H3
OB	17-19	H5a, H5b, H5c, H5d
AH	20-23	H4a, H4b
CB	24	H6a, H6b, H6c, H6d
Actual UXA Compliance	n/a	H7a, H7b, H8a, H8b
Age	25	

Reliability and Validity

Ifinedo (2012) evaluated composite reliability, convergent validity, and discriminant validity for the instrument questions. Composite reliability for all items exceeded the recommended statistical measure of 0.7 (Ifinedo, 2012). Convergent validity was tested by Average Variance Extracted (AVE) and all items exceeded the 0.5 standard statistical cutoff (Ifinedo, 2012). Discriminant validity was tested by AVE and

square root of AVE being greater than the cross correlations (Ifinedo, 2012). Again, all items were found to meet this requirement.

Siponen et al. (2014) tested convergent validity, internal consistency, and composite reliability. For convergent reliability they evaluated factor loading and all items exceeded 0.69 (Siponen et al., 2014). All items scored greater than the statistical cutoff of 0.5 for variance extracted (Siponen et al., 2014). To test internal consistency, Cronbach's α was used, and all items exceeded 0.6 (Siponen et al., 2014). For composite reliability, all items exceeded the cutoff of 0.7 (Siponen et al., 2014). Finally, discriminant validity was tested via inter-item correlations and all were below the statistical cutoff of 0.9 (Siponen et al., 2014).

Hanus and Wu (2016) tested the reliability of their items using Cronbach's α and all measured greater than 0.7. Convergent validity was tested using AVE and all items exceeded the 0.5 statistical requirement (Hanus & Wu, 2016). Discriminant validity was tested using cross loadings and Fornell-Larcker criterion and all exceeded the statistical requirements for inclusion (Hanus & Wu, 2016).

Safa et al. (2016) evaluated convergent validity, internal consistency, and discriminant validity for their model's items. Factor loading was used to evaluate convergent validity and all items above the 0.5 statistical cutoff were included (Safa et al., 2016). Internal consistency was tested with Cronbach's α and all items exceeded 0.7 (Safa et al., 2016). Discriminant validity was tested using inter-item correlations and all were below the 0.9 statistical cutoff (Safa et al., 2016). Additionally, all variances exceeded the recommendation of 0.5 (Safa et al., 2016). Finally, the square root of the AVE exceeded all correlations further indicating the discriminant validity (Safa et al.,

2016).

Rhee et al. (2012) tested their instrument for reliability, convergent validity, and discriminant validity. Reliability was assessed by identifying the composite reliability (0.908) and AVE (0.925) both of which exceeded the standard cutoff of 0.7 and 0.5 respectively (Rhee et al., 2012). Convergent validity was tested by evaluating all item loadings, which all exceeded 0.73 (Rhee et al., 2012). Finally, discriminant validity was verified by using the square root of all AVEs and comparing them to the correlations between factors (Rhee et al., 2012). Again, all items met the criteria for discriminant validity.

Variables

Threat Appraisal

Threat appraisal is an evaluation of the UXA TA-PS and TA-PV to IS threats (Posey et al., 2015; Rogers & Prentice-Dunn, 1997). TA-PV and TA-PS may be influenced by cognitive heuristics, which may be influenced by an increased knowledge and awareness of IS risks and vulnerabilities (Albrechtsen & Hovden, 2010; Guo et al., 2011; Safa & Von Solms, 2016; Siponen et al., 2014). TA-PS and TA-PV were assessed via three survey questions each adapted from Ifinedo (2014) and Hanus and Wu (2016).

Coping Appraisal

Coping appraisal is an assessment of how the UXA perceives that they can cope with, adapt to, or mitigate the IS risk (Rogers & Prentice-Dunn, 1997). Coping appraisal considers the UXA's IS CA-SE and IS CA-RE (Posey et al., 2015). CA-RE is an assessment of how effective the proposed behavior can reduce the probability of the negative event (Rogers & Prentice-Dunn, 1997). CA-SE is the belief that one can make

the changes needed to mitigate the risk (Rogers & Prentice-Dunn, 1997). CA-SE and CA-RE were assessed by three questions each that were adapted from Ifinedo (2014) and Hanus and Wu (2016).

Cognitive Heuristics

The cognitive heuristics that were evaluated included the AH, OB, and CB. The use of these heuristics can influence UX A estimation of risk and vulnerability associated with their UNIX servers (Kahneman, 2011; Pachur et al., 2012; Tversky & Kahneman, 1974). Additionally, OB, and CB may influence UX A coping appraisal. The AH was measured by four questions that ask participants to evaluate vulnerability and exploitability of UNIX and Windows servers (Kahneman, 2011; Kliger & Kudryavtsev, 2010; Tversky & Kahneman, 1974). OB was assessed using three questions from Rhee et al. (2012). Confirmatory bias was tested using a fictional scenario, similar to the technique of Fischer et al. (2011) where participants are presented a scenario, asked to make an initial decision, then provided six confirming and six disconfirming bits of additional information they can choose to review, and then asked to choose again. The level of CB was determined by subtracting the number of disconfirming choices selected from the confirming choices selected (Fischer et al., 2011; Gertner et al., 2016).

ISP Compliance Behavior

UX A ISP compliance behavior was assessed by analyzing six percentages for specific security implementations for all the UNIX servers managed by each UX A. Percentages are frequently used for analyzing and presenting security metrics as they are easily interpretable and can clearly indicate positive or negative change (Brotby & Hinson, 2013; Hayden, 2010; Hubbard & Seirsens, 2016; Jaquith, 2007). Table 3 identifies

the data points collected and the associated PLS-SEM coding.

Table 3

<i>ISP Behavioral Data Points</i>	
Data point	PLS-SEM Code
Percentage of administrator's servers sending data to centralized log management system.	COMPL1
Percentage of administrator's servers with centrally recorded Tenable Nessus data.	COMPL2
Percentage of administrator's servers blocking telnet/ftp ports (TCP/UDP 21, 23) and remote services ports (TCP/UDP 512-514).	COMPL3
Percentage of an administrator's servers using multi-factor authentication.	COMPL4
Percentage of an administrator's servers that have had recent software updates.	COMPL5

The percentage of administrator's servers sending data to centralized log management system (COMPL1) was determined from a report provided by the IS team's Splunk administrator. This report identified all servers, UXAs, on-call groups, and projects for all servers sending data to the Splunk log management servers. Servers were associated with the specific UXA and percentages were determined based on CMDB data. The percentage of administrator's servers with centrally recorded Tenable Nessus data (COMPL2) was determined by using the organization's Tenable Splunk dashboard filtered by each UXA. The dashboard provides a listing of the Tenable hosts and hosts not in a scan group for each administrator. Counts were input into an Excel spreadsheet and percentages computed for each UXA. The percentage of administrator's servers blocking telnet, ftp, and remote services ports (COMPL3) was determined by running a script that programmatically performed nmap scans on the specific ports for each server identified in the CMDB for each UXA. The script indicated the servers that were processed, as well as an indication of whether the ports were open, closed, or filtered. Ports that identified as

filtered indicate the presence of a firewall or other filter securing the port (NMAP.ORG, 2019). This script was run in batches of 100 servers to minimize the network impact. Again, servers were associated with the appropriate UXA based on the CMDB. The percentage of an administrator's servers using multi-factor authentication (COMPL4) was determined by identifying all UNIX servers registered with PAM RADIUS secrets in the organization's multifactor authentication database. These data, made available by the IS team, indicated server, IP address, managing group, as well as the associated PAM RADIUS secrets. Server hostnames were matched to the corresponding UXA to tally a total and determine the percentage. The percentage of an administrator's servers that have had recent software updates (COMPL5) was determined using two methods. For all Linux servers, the organization's Splunk Linux Inventory Dashboard was modified to provide a listing of kernel packages installed on the Linux servers. This database was queried prior to the workshop as a baseline and then again 90 days after the workshop. For IBM AIX servers a script was developed which queried the server's installed software and determined dates for all installed software packages. Servers were associated with specific UXAs and percentages were calculated for each UXA. Data points were collected for each UXA prior to and 90 days following the workshop and recorded in an Excel spreadsheet. Using security scans, security reports, and authenticated scripts to identify the security measures implemented by UXA following the SETA workshop afforded unique insights into the effectiveness of the training in terms of actual implementation of security controls and ISP compliance behavior.

Population and Sampling

After IRB approvals (Appendix G), the IS team identified the subject pool made

up of all UXAs in the organization. Email invitations were sent to all potential participants inviting them to participate in the workshop (Appendix H). Reminder emails were sent to individuals that had not responded (accepted or declined) the invitation. Individuals that chose to participate received an email link for informed consent (Appendix I). Once informed consent was received a link to the Qualtrics survey was emailed to participants. Reminder emails were sent to individuals to complete the survey. The 60 individuals participated in the SETA workshop via a secure Zoom meeting. The workshop lasted 2.5 hours and focused on increasing cybersecurity awareness and cyber skills related to UNIX servers in a healthcare organization.

The day of the workshop, individual emails were sent to each participant providing them login information and for the ISC (Appendix J). After completion of the workshop, participants were introduced to the EDURange environment, instructed how to access it, and were provided with login information related to the ISC. Participants began connecting to the EDURange scenario and started the ISC, which was available for five hours following the workshop. This scenario provided participants a hands-on experience using tools introduced in the workshop (nmap and Metasploit) to identify, enumerate, and exploit the vulnerable Linux VM in the EDURange platform. At the request of several participants, the ISC was restarted and made available to the participants the following day so that they could continue. Finally, at the request of several additional participants, the ISC was restarted again one month after the workshop to allow participants to continue to utilize the platform.

After the workshop, security update emails were sent to the participants to maintain cyber awareness and reinforce the materials presented in the workshop. The

emails were sent at week 1, 4, 7, and 10 following the workshop. The content of the updates included information about newly identified vulnerabilities, CERT alerts, organizational breach updates, external breach reports, InfraGard updates, relevant security news, and an invitation to participate in the newly created Microsoft Teams collaborative group. The focus of these updates was to continue to increase UXAs awareness of the vulnerabilities and how best to mitigate risk for their servers.

Three months after the workshop, an email was sent to all participants requesting they complete the Qualtrics survey a second time. Reminder emails were sent to individuals to complete the second survey. Additionally, security implementation data were collected for all servers associated with each UXA to quantify the changes made during the study.

The population was made up of the UXAs in a major university and hospital system in the mid-Atlantic United States. The organization manages more than 1000 UNIX physical and logical servers located in four data centers in two states as well as the District of Columbia. The UXAs are responsible for the servers running enterprise wide applications including the electronic medical record system, pathology labs, radiology, Web services, IS servers, student information systems, precision medicine systems, document management system, change control systems, as well as numerous departmental systems that house PHI and PII. Presently there are 60 UXAs across the organizations.

Sampling Method

A listing of all active UXAs was obtained from the IS manager within the organization. As only 60 individuals were identified, they were all invited to participate in

the workshop.

Study Participants

The UXAs in the organization are made up of individuals with a wide variety of technical experience and educational background. The workshop included sixty participants. Thirty participants identified primarily UNIX server administrators. Some (12) participants identified as split responsibility for both UNIX and Windows servers. Four participants identified themselves as Windows-only server administrators; seven workshop participants did not have any responsibility for servers; seven individuals did not complete all the study protocols. These 18 participants were removed from the study. A total of 42 participants completed all the study protocols. One participant was female, and 41 participants were male (Table 4). This is not unusual given the gender imbalance noted in IT (Gorbacheva et al., 2019). Most participants were aged 45-65 (52.4%). Remaining ages included 35-44 (26.2%), 25-34 (16.7%), and 66+ (2.4%) (Table 5). Regarding education attainment for the participants, 26.2% have graduate degrees, 50.0% have bachelor's degrees, 11.9% have associate degrees, and 11.9% have some college but no degree (see Table 6).

Table 4

<i>Participant Gender (N=42)</i>		
Gender	Count	Percentage
Male	41	97.60%
Female	1	2.40%

Table 5

Participant Age (N=42)

Age	Count	Percentage
17-24	1	2.40%
25-34	7	16.70%
35-44	11	26.20%
45-65	22	52.40%
66+	1	2.40%

Table 6

Participant Education (N=42)

Age	Count	Percentage
High school	0	0%
Some college (no degree)	5	11.90%
Associates degree	5	11.90%
Bachelor's degree	21	50.00%
Graduate degree	11	26.20%

Data Collection

Two types of data were collected. First, the survey instrument was used prior to and 90-days following the intervention. The survey request was sent via email and was administered online using Qualtrics. The survey consisted of 25 questions and measures the following constructs: CA-SE, CA-RE, TA-PV, TA-PS, ISKS, AH, OB, and CB. The second set of data points were an analysis of security controls implemented on each UXAs servers. Security scans and scripts were run on all UNIX servers associated with each participant prior to and three-months following the workshop and ISC. Jaquith (2007) recommended quarterly analysis of security metrics as they provide necessary precision for a time series-based analysis of security implementations. Quarterly analysis allowed for analysis of the ISP compliance by evaluating the security changes

implemented by each UXA.

Survey results were downloaded from Qualtrics into a spreadsheet. UXAs were assigned a unique ID and all results associated with that UXA were coded with that unique ID. These codes helped to ensure anonymity of responses while still allowing for the connection of the ISP compliance behavior data points to the specific UXA by the researcher. The compliance data were collected for all servers managed by each UXA and entered into the study spreadsheet.

Data Analysis

Partial least squares structural equation modeling (PLS-SEM) has been used extensively to test complex models in IS (Hanus & Wu, 2016; Ifinedo, 2012; Rhee et al., 2012; Safa & Von Solms, 2016; Safa et al., 2016). PLS-SEM has characteristics that demonstrate its utility in the present research including acceptance of small sample sizes, no assumption of data normality, variety of scales of measurement, and ability to handle complex models (Hair et al., 2017). Hair et al. (2017), indicate that at a significance level of 5% with maximum of three arrows pointing toward a construct (Threat Appraisal), a minimum R^2 of 0.25 requires a 33-participant sample size and a minimum R^2 of 0.50 requires 14 participants (p. 26). PLS-SEM evaluated an inner model or structure using path coefficients and an outer model, also termed the measurement model, with the factors used to represent the latent variables (Hair et al., 2017). PLS-SEM allowed for the examination of the paths of the model as well as the relationships between the variables (Hanus & Wu, 2016; Safa & Von Solms, 2016). SmartPLS 3.2.8 was used to perform analyses of the data. SmartPLS provided reports of the following: Cronbach's α , average variance explained, Average Variance Extracted (AVE), Fornell-Larcker criterion, and R^2

for testing the outer and inner models (Hair et al., 2017). Figure 3 is an illustrated initial layout of SmartPLS for the proposed model.

The measurement model was assessed for internal consistency reliability, indicator reliability, convergent validity, and discriminant validity (Hair et al., 2017). The structural model was assessed for collinearity among the constructs, relevance and significance of the path coefficients, predictive relevance, predictive model selection, and goodness-of-fit (Hair et al., 2017). Internal consistency reliability was evaluated with Cronbach's α . Values greater than 0.60 indicated internal consistency reliability for all new constructs while established constructs should have values greater than 0.70 (Hair et al., 2017). Composite reliability was assessed with ρ . Levels greater than 0.70 indicated composite reliability. Indicator reliability was assessed by using the outer loadings provided by SmartPLS. The indicators outer loading indicates the correlation between the construct and the specific indicator. The explained variance was calculated by squaring the outer loading and results should be larger than 0.7 to show indicator reliability (Hair et al., 2017).

Convergent validity was assessed using the Average Variance Extracted (AVE). The AVE is a grand mean made up of the squared loadings for all the indicators associated with the specific construct (Hair et al., 2017). AVE was calculated for each construct using the indicator loadings, squared, and then averaged. Hair et al. (2017) indicated that each construct should have $AVE \geq 0.50$. Outer loading relevance was tested by evaluating the outer loading scores from SmartPLS. For values ≥ 0.70 the indicator was retained (Hair et al., 2017). For outer loadings between 0.40 and 0.70 the data were reanalyzed to determine the impact of the indicator deletion on the AVE and

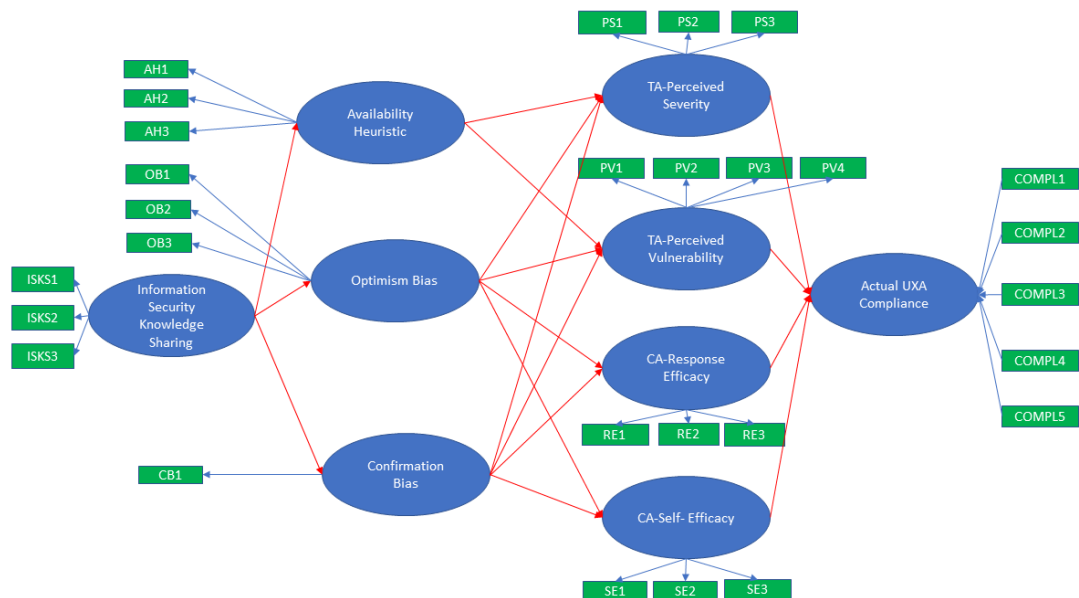
composite reliability (Hair et al., 2017). For outer loadings below 0.40 the reflective indicator was removed from the model (Hair et al., 2017). Discriminant validity was calculated to determine if the constructs are conceptually and statistically distinct (Hair et al., 2017). To assess discriminant validity of the reflective measurement models, Heterotrait-Monotrait Ratio (HTMT) was used. Henseler et al. (2015) found HTMT to be more effective in identifying problems with discriminant validity than the more popular Fornell-Larcker criterion. The threshold suggested by Kline (2011) is 0.85.

To analyze the structural model, the model was evaluated for collinearity, the significance and relevance of the relationships in the structural model were assessed, and the predictive relevance of the model was assessed (Hair et al., 2017). Collinearity was assessed using the variance inflation factor (VIF) (Hair et al., 2017). VIF values were used to determine if a critical level of collinearity occurred. VIF values below 5 or better below 3 indicate that the level of collinearity is acceptable (Hair et al., 2017). Path coefficients were evaluated to determine their significance and relevance (Hair et al., 2017). The types of effects analyzed included the direct effects, indirect effects, and total effects. Path coefficients range from -1 to 1. Significance of the effects were evaluated using bootstrapping (Hair et al., 2017). Finally, the predictive relevance of the model was assessed by analyzing the out-of-sample and in-sample predictions (Hair et al., 2017). In-sample prediction, or explanatory power, was assessed using the entire dataset less a holdout sample, to estimate the model and predict observations using the coefficient of determination (R^2) and effect size (Hair et al., 2017). R^2 values range from 0 to 1 where below 0.25 is weak, 0.5 is moderate, and .75 is substantial (Hair et al., 2017). The effect size is used to determine how one construct contributes to the explaining power of

another construct (Hair et al., 2017). An effect size value from 0.02 to 0.15 is considered weak effect, from 0.15 to 0.35 is a moderate effect, and greater than 0.35 is considered a strong effect (Hair et al., 2017). Out-of-sample prediction, or predictive power, was assessed to predict observations in a holdout sample using blindfolding-based Q2 (Hair et al., 2017). In blindfolding the model is computed iteratively while systematically omitting some of the data points (Hair et al., 2017). Model estimates that are created using the sample data are used to predict the omitted data (Hair et al., 2017). Predictive relevance is determined by assessing the predictive error (Hair et al., 2017). Q² results from 0.02 to 0.15 indicates weak predictive power, values between 0.15 and 0.35 indicates moderate predictive power, and values greater than 0.35 indicates strong predictive power (Hair et al., 2017).

Figure 3

SmartPLS Model Layout



Comparisons of pre-intervention and post-intervention statistics were completed using dependent-sample t-tests. T-tests allow for comparison of means and as this is a

before and after comparison, the samples were dependent on one another (Terrell, 2012). Microsoft Excel's Statistics package was used to compute the critical t values used to determine if the compliance metrics were statistically different between the pre-workshop analysis and the analysis performed 90-days after the workshop. Additionally, descriptive statistics (mean, standard deviation, skewness, and kurtosis) were calculated for all the constructs.

Format for Presenting Results

Based on the results of the statistical analyses, a report was developed and presented as chapter four of the dissertation report (Terrell, 2016). The analyses included narrative form, diagrams, and tables related to survey administration, survey questions and responses, demographics of participants, pre and post intervention server analyses and results, workshop feedback/analysis, ISC feedback/results, PLS structural and measurement model analysis, hypotheses testing results, and proposed answers to the research question. The data included, where applicable, quantitative descriptive statistics. The PLS-SEM structural analysis included data related to the collinearity assessment, relevance and significance of path coefficients, predictive relevance, and goodness of fit. The PLS-SEM measurement model data included a report of the convergent and discriminant validity, internal consistency reliability, indicator reliability, and composite reliability. PLS-SEM data were presented via diagram, table, and narrative to explain the results. Other quantitative data were presented in tabular form. Finally, chapter five provides conclusions based on the analysis, a summary of implications for UX A SETA training, as well as recommendations for future research.

Resources

Required resources fell into three categories: administration, people, and technology. Administratively, the study proposal was defended, and IRB requests were submitted to both institutions. The IRB review process at the workshop site took almost six weeks of revisions. Support from the C-Suite for the research was already secured. In terms of people, participation of a diverse set of UXAs across the organization was required. Technology requirements included access to Qualtrics for survey administration, development of and access to EDURange for the ISC, SmartPLS for PLS-SEM statistical analyses, participants' access to networked computers, access to the organization's configuration management database, access to the organization's Tenable servers, access to the Splunk dashboards, access to the MFA database, and the ability to run scripts and scans on the UXAs' servers. A new EDURange scenario was developed, in coordination with the EDURange team that consisted of an ISC module to provide hands-on SETA for UXAs.

Summary

This quantitative study was conducted in a pretest and posttest experimental and control group design and evaluated the effectiveness of a SETA workshop, ISC, and periodic security update emails on the ISP compliance of UXAs. The survey instrument was developed based on prior validated instrument questions augmented with newly designed questions related to the use of cognitive heuristics and biases. The survey was completed by participants prior to and following the workshop and ISC. Compliance behavior was assessed using security scans and evaluation of specific metrics directly tied to the SETA workshop and ISC learning objectives. SmartPLS was used to analyze the

data and evaluate the structural and measurement model proposed. Dependent t-tests were used to analyze the behavioral data to evaluate the potential differences between pre- and post-intervention actual UXA compliance.

Chapter 4

Results

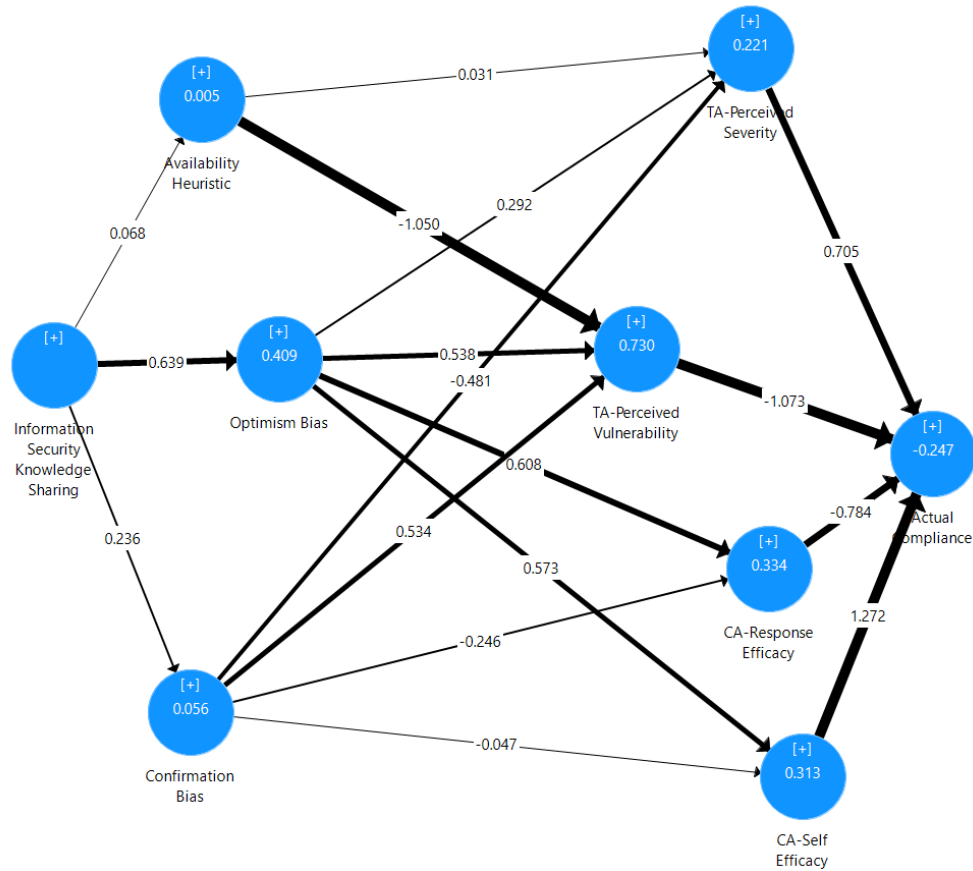
Overview

This chapter provides the data analyses of the pre-workshop survey and behavioral metrics, as well as the post-workshop survey and behavioral metrics. The survey and server analyses results were analyzed in two phases. The theorized model and indicators were entered into SmartPLS. Once data were collected for the pre-workshop survey and compliance metrics, they were entered into SmartPLS. Initial evaluation of the measurement model and structural model were completed on the pre-workshop data. After 90 days, the post-workshop survey data and compliance metrics were collected and a second SmartPLS analysis was performed. Additionally, descriptive statistics were performed to evaluate the changes between the pre-workshop and post-workshop compliance metrics to determine if significant changes were made in behavior as a result of the intervention. The results of these analyses are indicated below. Following the data analyses, findings and a summary close out this chapter of the dissertation report.

Data Analysis

The process for performing an analysis of a new model, as outlined by Hair et al. (2017), included the following steps: creation of the structural model, creation of the measurement models for each construct, collection/examination of data, estimation of the PLS path model, assessment of the (reflective) measurement model, and finally assessment of the structural model. The model, based on prior research, was created in SmartPLS. The data from the survey were exported from Qualtrics to a Microsoft Excel

spreadsheet. AC security metrics were collected from scripts, Tenable Nessus, Splunk, and organizational data. Results for these data points were aggregated and stored in a Microsoft Excel spreadsheet. The compliance data were merged with the survey data to provide a single comma delimited file for input into SmartPLS. Preliminary evaluation of the data using a consistent PLS algorithm indicated several unexpected results. A deeper dive into the data showed that there were several individuals whose responses were significantly different from others in the sample data. Through conversations with those participants it was discovered that several participants were Windows server administrators not UXAs. Since the focus of this study was on the unique UXA cognitions, the Windows server administrators were removed from the data. The SmartPLS analysis for data prior to the workshop and ISC is shown in Figure 4.

Figure 4*Pre-workshop PLS-SEM Analysis Results*

The pre-workshop measurement model was assessed for internal consistency reliability, indicator reliability, convergent validity, and discriminant validity (Hair et al., 2017). The structural model was assessed for collinearity among the constructs, as well as relevance and significance of the path coefficients (Hair et al., 2017).

Internal consistency reliability was evaluated with Cronbach's α . Values greater than 0.60 indicated internal consistency reliability for all new constructs while established constructs should have values greater than 0.70 (Bagozzi & Yi, 1988; Hair et al., 2017; Henseler et al., 2016). The pre-workshop Cronbach's α indicated that CA-CA-

RE, CA-SE, CB, ISKS, OB, and TA-PS achieved the required cutoffs for new constructs and existing constructs (Table 7). The AH, and TA-PV, however, failed to meet the Cronbach's α cutoff. Three TA-PV survey questions were derived from Hanus and Wu (2016), Siponen et al. (2014), and Ifinedo (2012) as well as one question that was developed based on the recommendation of a pilot-tester. It is theorized that, while the four questions seemed to be pertinent and collectively represent this construct for the current study, taken individually there were inconsistencies that resulted in the lower Cronbach's α than had all of the survey question come from a single instrument. The AH survey questions were developed for this study. VIF and HTMT were evaluated and all the indicators met collinearity constraints. Clearly, however, the questions associated with AH need to be reevaluated.

Table 7

<i>Pre-workshop Cronbach's α (N=42)</i>	
Construct	Cronbach's α
AH	0.403
CA-RE	0.661
CA-SE	0.856
CB	1
ISKS	0.683
OB	0.691
TA-PS	0.867
TA-PV	0.419

Composite reliability of the pre-workshop data was assessed with ρ . Levels greater than 0.70 indicated composite reliability for established constructs while values greater than 0.60 are acceptable for exploratory research (Henseler et al., 2016; Wong, 2019). AC, AH, CA-RE, CA-SE, CB, ISKS, OB, and TA-PS met ρ significance levels (Table 8). TA-PV, however, was well below the required cutoff point. Again, it was

theorized that pulling single questions from different scales may have resulted in the failure of TA-PV to meet demonstrate composite reliability.

Table 8

<i>Pre-workshop ρ (N=42)</i>	
Construct	ρ
AC	1
AH	0.771
CA-RE	0.7
CA-SE	0.858
CB	1
ISKS	0.768
OB	0.739
TA-PS	0.896
TA-PV	0.251

Convergent validity was assessed using the AVE. The AVE is a grand mean made up of the squared loadings for all the indicators associated with the specific construct (Hair et al., 2017). The AVE was calculated in SmartPLS (Table 9). Six constructs met the AVE level of significance CA-RE (0.585), CA-SE (0.774), CB (1.00), ISKS (0.571), OB (0.612), and TA-PS (0.79). AH and TA-PV did not meet the critical cutoff for significance. To further assess AVE, the bootstrapped AVE was calculated for each construct (PLS algorithm max number of iterations: 5000; bootstrapping settings: complexity: complete bootstrapping, samples: 5000, significance: 0.05, test type: one tailed) (Hair et al., 2017). As noted in Table 10, the bootstrapped AVEs for all constructs were significant ($p < 0.05$).

Table 9

Pre-workshop AVE (N=42)

Construct	AVE
AH	0.442
CA-RE	0.585
CA-SE	0.774
CB	1
ISKS	0.571
OB	0.612
TA-PS	0.79
TA-PV	0.397

Table 10

Pre-workshop Bootstrapped AVE (N=42)

Construct	Original Sample	<i>M</i>	<i>SD</i>	<i>t</i>	<i>p</i>
AH	0.442	0.453	0.065	6.818	< 0.001
CA-RE	0.585	0.549	0.118	4.968	< 0.001
CA-SE	0.774	0.764	0.085	9.052	< 0.001
ISKS	0.571	0.563	0.108	5.274	< 0.001
OB	0.612	0.607	0.062	9.812	< 0.001
TA-PS	0.79	0.776	0.086	9.139	< 0.001
TA-PV	0.397	0.408	0.067	5.924	< 0.001

Discriminant validity was calculated to determine if the constructs are conceptually and statistically distinct (Hair et al., 2017). To assess discriminant validity of the reflective measurement models, Heterotrait-Monotrait Ratio (HTMT) was used. Henseler et al., (2015) found HTMT to be more effective in identifying problems with discriminant validity than the more popular Fornell-Larcker criterion. The HTMT table was evaluated to determine if the correlations within values are greater than the correlations across the model (Henseler et al., 2015). Threshold values should be 0.85 (Kline, 2011; Wong, 2019) or a more liberal cutoff of 0.90 can be used (Gold et al., 2001). Based on the results from SmartPLS, the HTMT values for all constructs met the desired cutoff indicating discriminant validity (Table 11).

Table 11*Pre-workshop HTMT (N=42)*

Construct	AH	CA-RE	CA-SE	CB	ISKS	OB	TA-PS	TA-PV
AH								
CA-RE	0.49							
CA-SE	0.452	0.837						
CB	0.489	0.103	0.237					
ISKS	0.354	0.773	0.733	0.262				
OB	0.623	0.539	0.554	0.311	0.652			
TA-PS	0.265	0.487	0.236	0.373	0.371	0.179		
TA-PV	0.409	0.563	0.431	0.345	0.494	0.37	0.474	

To analyze the pre-workshop structural model, the model was evaluated for collinearity, as well as the significance and relevance of the relationships (Hair et al., 2017). Collinearity was assessed using the VIF (Hair et al., 2017). Constructs with high collinearity indicate that there is a high degree of redundancy and correlation between two or more predictor variables (Hair et al., 2017). VIF values below five indicate that the level of collinearity is acceptable (Hair et al., 2017; Wong, 2019). Table 12 from SmartPLS shows that all constructs met the statistical cutoff for collinearity. The highest VIF values was for CA-RE->AC (3.099) indicating there is a degree of correlation between the indicators but that they do not reach the level where statistical significance was in question.

Table 12

Pre-workshop Inner VIF (N=42)

Construct	AC	AH	CA-RE	CA-SE	CB	ISKS	OB	TA-PS	TA-PV
AC									
AH								1.619	1.619
CA-RE	3.099								
CA-SE	-1.491								
CB			1.115	1.115				1.339	1.339
ISKS		1			1		1		
OB			1.115	1.115				1.36	1.36
TA-PS	-1.207								
TA-PV	-3.418								

Path coefficients were evaluated to determine their significance and relevance (Hair et al., 2017; Wong, 2019). The types of effects analyzed included the direct effects, indirect effects, and total effects. Path coefficients range from -1 to 1. The direct effect was determined using the path effect between linked constructs. Path coefficients provide an indication of how much a dependent variable will change based on an independent variable. For a one standard deviation change of the independent variable the dependent variable will change x (path coefficient) standard deviations (Hair et al., 2017). With regard to AC, CA-SE had the highest positive impact (1.272), and TA-PS was also significant (0.705) (Table 13). TA-PV (-1.073) and CA-RE (-0.784) had significant negative effects on AC. With respect to the three evaluated cognitive heuristics and biases, the AH had a significant negative impact on TA-PV (-1.050), while OB (0.538), and CB (0.534) had significant positive impacts on TA-PV. This implies that the greater the use of the AH results in a greater sense of invulnerability. Interestingly, based on the pre-workshop results, the use of confirmation bias and OB increase TA-PV. TA-PS was negatively influenced by CB (-0.481) and positively influenced by OB (0.292) and AH (0.031). From a CB perspective this seemed logical as using the bias resulted in reduced

perceived threat awareness and TA-PS. The positive path coefficient between OB and TA-PS implies that when the bias is used, TA-PS is increased slightly. CA-RE is most positively influenced by OB (0.608) and is negatively influenced by CB (-0.246). This seemed logical given that the use of OB implied higher level of belief of invulnerability and this could extend to the perception that CA-RE was high as well. The negative relationship between CB and CA-RE (-0.246), indicated that individuals who are using CB tend to believe their ability to respond to security risks is reduced. CA-RE is most highly impacted by OB (0.573) and negatively impacted by CB (-0.047). Again, this seemed appropriate since the use of OB would artificially inflate the sense of CA-SE of the UXAs. OB was most highly positively influenced by ISKS (0.639). This evaluation was done prior to the workshop and it seems logical that a positive sense of information sharing results in a greater degree of optimism about the security of one's UNIX servers. CB was also positively influenced by ISKS (0.236). Since, when wielding CB, one is looking for information that supports your strongly held beliefs, this scoring was not surprising. There was only a minimal positive influence of ISKS on the AH (0.068). The use of the AH relates to the sense of how easily one recalls information related to a specific question. These results indicated that increased ISKS can result in minimal increase in AH.

Table 13

Pre-workshop Path Coefficients (N=42)

Construct	AC	AH	CA-RE	CA-SE	CB	ISKS	OB	TA-PS	TA-PV
AC									
AH								0.031	-1.05
CA-RE	-0.784								
CA-SE	1.272								
CB			-0.246	-0.047				-0.481	0.534
ISKS		0.068			0.236		0.639		
OB			0.608	0.573				0.292	0.538
TA-PS	0.705								
TA-PV	-1.073								

Indirect effect was evaluated by looking at additional paths between constructs through at least one other construct (Table 14). The most significant positive indirect effect was on the AH on AC (1.149). The use of CB had a significant negative effect (-0.778) on AC. OB had a small negative effect (-0.120) on AC. ISKS had a small negative effect on AC but a positive effect on TA-PV, CA-SE, CA-RE, and TA-PS (in order of effect). It seemed logical that ISKS would have a positive effect on CA-RE, CA-SE, TA-PS, and TA-PV given that security education generally increases participants ability to identify and respond to risks and vulnerabilities. The negative influence of ISKS on AC was puzzling and was theorized to be less relevant given the ISKS intervention had not yet occurred (the workshop).

Table 14

Pre-workshop Indirect Effects (N=42)

Construct	AC	AH	CA-RE	CA-SE	CB	ISKS	OB	TA-PS	TA-PV
AC									
AH	1.149								
CA-RE									
CA-SE									
CB	-0.778								
ISKS	-0.183		0.33	0.355				0.075	0.399
OB	-0.12								
TA-PS									
TA-PV									

Specific indirect effects were analyzed from SmartPLS (Table 15). The most significant negative specific indirect effects on compliance included: OB->TA-PV->AC (-0.577), CB->TA-PV->AC (-0.573), OB->CA-RE->AC (-0.476), ISKS->OB->TA-PV->AC (-0.369), CB->TA-PS->AC (-0.339), ISKS->OB->CA-RE->AC (-0.305). The most significant positive specific indirect effects on compliance included: AH->TA-PV->AC (1.127), OB->CA-SE->AC (0.728), ISKS->OB->CA-SE->AC (0.465). In terms of other specific indirect effects ISKS->OB->CA-RE (0.389), ISKS->OB->CA-SE (0.366), and ISKS->OB->TA-PV (0.344) were all significant. The indirect effects indicate that CB, OB, and AH all played a significant role in AC.

Table 15

<i>Pre-workshop Specific Indirect Effects (N=42)</i>	
Path	Specific Indirect Effects
CB->CA-RE->AC	0.193
ISKS->CB->CA-RE->AC	0.046
OB->CA-RE->AC	-0.476
ISKS->OB->CA-RE->AC	-0.305
CB->CA-SE->AC	-0.06
ISKS->CB->CA-SE->AC	-0.014
OB->CA-SE->AC	0.728
ISKS->OB->CA-SE->AC	0.465
AH->TA-PS->AC	0.022
ISKS->AH->TA-PS->AC	0.002
CB->TA-PS->AC	-0.339
ISKS->CB->TA-PS->AC	-0.08
OB->TA-PS->AC	0.206
ISKS->OB->TA-PS->AC	0.131
AH->TA-PV->AC	1.127
ISKS->AH->TA-PV->AC	0.076
CB->TA-PV->AC	-0.573
ISKS->CB->TA-PV->AC	-0.135
OB->TA-PV->AC	-0.577
ISKS->OB->TA-PV->AC	-0.369
ISKS->CB->CA-RE	-0.058
ISKS->OB->CA-RE	0.389
ISKS->CB->CA-SE	-0.011
ISKS->OB->CA-SE	0.366
ISKS->AH->TA-PS	0.002
ISKS->CB->TA-PS	-0.113
ISKS->OB->TA-PS	0.186
ISKS->AH->TA-PV	-0.071
ISKS->CB->TA-PV	0.126
ISKS->OB->TA-PV	0.344

The total effect was analyzed based on the results of the SmartPLS run (Table 16).

The most significant positive influencers on AC were CA-SE (1.272), AH (1.149), and TA-PS (0.705). CA-SE and TA-PS are known to have a positive relationship with compliance intention but the finding that AH is a significant influencer is novel to the current study (Hanus & Wu, 2016; Vance et al., 2012). The most significant negative

influencers of AC included TA-PV (-1.073), CA-RE (-0.784), CB (-0.778), ISKS (-0.183), and OB (-0.120). CA-RE and CB may be explained due to the use of the bias skewing the UXAs belief that they need to comply with security directives. TA-PV's strong negative relationship may be due to UXAs perceiving the threat and feeling overwhelmed and unable to make significant changes to mitigate the threat.

Table 16

Pre-workshop Total Effects (N=42)

Construct	AC	AH	CA-RE	CA-SE	CB	ISKS	OB	TA-PS	TA-PV
AC									
AH	1.149							0.031	-1.05
CA-RE	-0.784								
CA-SE	1.272								
CB	-0.778		-0.246	-0.047				-0.481	0.534
ISKS	-0.183	0.068	0.33	0.355	0.236		0.639	0.075	0.399
OB	-0.12		0.608	0.573				0.292	0.538
TA-PS	0.705								
TA-PV	-1.073								

OB had a significant effect on CA-RE (0.608), CA-SE (0.573), TA-PV (0.538), and TA-PS (0.292). Since OB is an unwarranted belief that one is not in danger it seemed logical that this bias should influence CA-RE, CA-SE, TA-PV, and TA-PS. CB had a significant negative effect on AC (-0.778), TA-PS (-0.481), and CA-RE (-0.246). Since CB may lead UXAs to only see information that supports their strongly held opinions it is not surprising that increases in CB result in less compliance, less TA-PS, and less CA-RE. ISKS had a positive influence on OB (0.639), TA-PV (0.399), CA-SE (0.355), CA-RE (0.330), and CB (0.236) and a minimal positive effect on TA-PS (0.075) and AH (0.068). These findings are in line with prior research that found that ISKS led to increased TA-PV, CA-SE, and CA-RE (Bélanger et al., 2017; Hanus & Wu, 2016; Posey et al., 2015). The findings related to OB and CB demonstrate the significant role each

plays in the model. CB had a significant positive influence on TA-PV (0.534). This may be caused by the increased use of the bias resulting in an invalid estimate of risk and an increase in TA-PV. CB had a negative influence on AC (-0.778), TA-PS (-0.481), CA-RE (-0.246), and CA-SE (-0.047). This indicated that, when the use of CB increased, compliance behavior, TA-PS, CA-RE, and CA-SE were all reduced. As noted earlier, this bias may blind the UXAs to the risks facing them. AH had a positive relationship with AC (1.149) and TA-PS (0.031) as well as a negative influence on TA-PV (-1.050). The negative influence on TA-PV indicates that the greater the use of the heuristic the lower the perceived danger facing the UXAs. The positive relationship between AH and AC (1.149) may indicate that the increase in security knowledge and awareness improved AC behavior. Clearly, based on the pre-workshop analysis, the increased use of AH resulted in increased compliance.

The significance of the path coefficients was evaluated using SmartPLS bootstrapping. This technique, in PLS, generates *t* statistics for both outer and inner models (Wong, 2019). The statistics were evaluated to determine if the path coefficients of the inner model were significant. The significant paths are indicated in Table 17 and included CB->TA-PS, ISKS->OB, OB->CA-RE, and OB->CA-SE.

Table 17

Pre-workshop Bootstrapped Path Coefficients (N=42)

Path	Original Sample	<i>M</i>	<i>SD</i>	<i>t</i>	<i>p</i>
CB->TA-PS	-0.378	-0.365	0.154	2.454	0.007**
ISKS->OB	0.594	0.596	0.123	4.81	<0.001***
OB->CA-RE	0.458	0.451	0.186	2.47	0.007**
OB->CA-SE	0.453	0.458	0.127	3.559	<0.001***

* $p < 0.05$; ** $p < 0.01$; *** $p < 0.001$

The effect size (f^2) is used to determine how one construct contributes to the explaining power of another construct (Hair et al., 2017; Wong, 2019). The effect sizes were computed using the PLS algorithm with quality criteria set to f-square (Table 18). An effect size value from 0.02 to 0.15 is considered weak effect, from 0.15 to 0.35 is a moderate effect, and greater than 0.35 is considered a strong effect (Hair et al., 2017). Strong positive effects included AH->TA-PV (2.522), CB->TA-PV (0.788), OB->TA-PV (0.788), ISKS->OB (0.691), OB->CA-RE (0.498), and OB->CA-SE (0.428). Moderate positive effects included CA-RE->AC (0.159), and CB->TA-PS and (0.222). Weak positive effects included CB->CA-RE (0.082), OB->TA-PS (0.080), and ISKS->CB (0.059). Strong negative effects included only CA-SE->AC (-0.869). Moderate negative effects included TA-PS->AC (-0.330), and TA-PV->AC (-0.270). As this evaluation was a baseline and done prior to the workshop and ISC it is not surprising that there were strong negative effects for CA-SE, TA-PS, and TA-PV on AC.

Table 18

<i>Pre-workshop Effect Size (N=42)</i>									
Construct	AC	AH	CA-RE	CA-SE	CB	ISKS	OB	TA-PS	TA-PV
AC									
AH								0.001	2.522
CA-RE	0.159								
CA-SE	-0.869								
CB			0.082	0.003				0.222	0.788
ISKS		0.005			0.059		0.691		
OB			0.498	0.428				0.08	0.788
TA-PS	-0.33								
TA-PV	-0.27								

Blindfolding was used to test predictive relevance using the Stone-Geisser values (Wong, 2019). Blindfolding systematically includes and omits some data points to

evaluate the model's ability to estimate/predict remaining points (Hair et al., 2017). To interpret blindfolding results, the Stone-Geisser's value (Q^2) between 0.02 and 0.15 indicated weak predictive power, between 0.15 and 0.35 indicated moderate predictive power, and greater than 0.35 indicated strong predictive power (Hair et al., 2017). CA-RE, CA-SE, and OB all had moderate levels of predictive power (Table 19). CB had weak predictive power. Other constructs predictive power were below 0.02 indicating little predictive power.

Table 19

<i>Pre-workshop Predictive Power (N=42)</i>		
Construct	Q²_predict	Predictive Power
CA-RE	0.175	Moderate
CA-SE	0.209	Moderate
CB	0.035	Weak
OB	0.278	Moderate

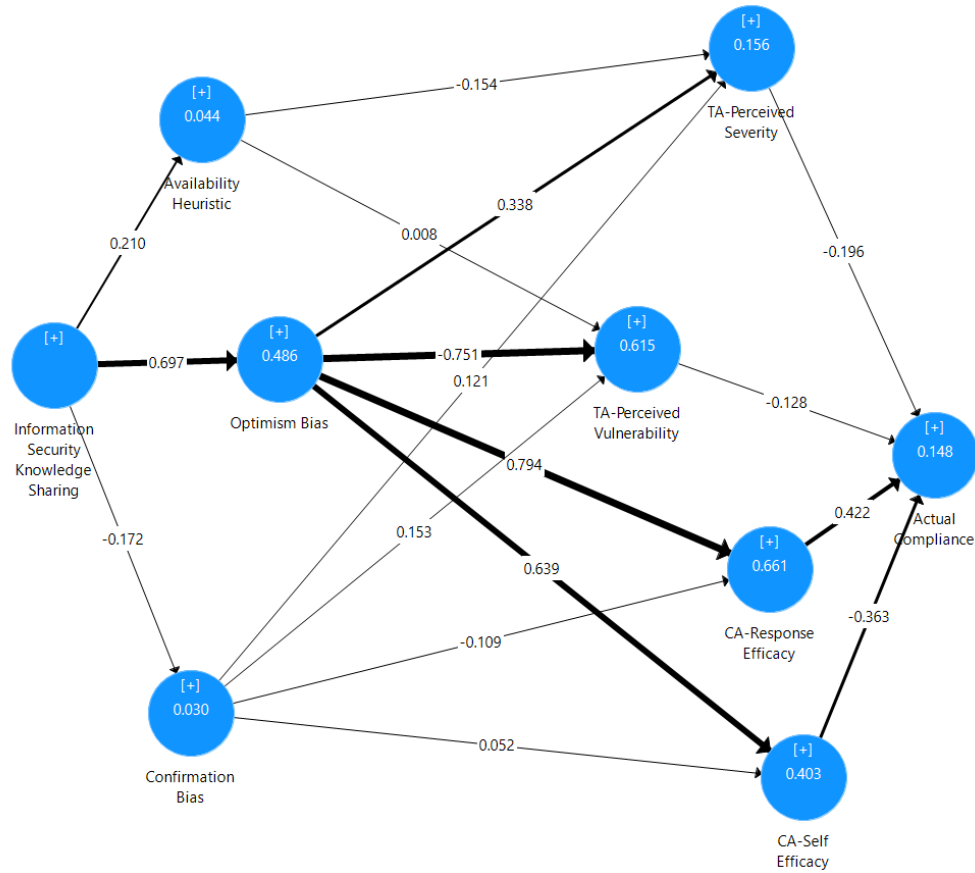
Following the workshop, ISC, and security update emails, the participants were asked to complete the survey a second time and data associated with their servers were collected. Ninety days were afforded to the UXAs to make changes to their servers in compliance with the ISP and by the direction of material in the workshop. The same model was used for the post-workshop analysis, but new responses were downloaded from Qualtrics and collected via script, Tenable Nessus, Splunk, or organization databases. Data were stored in Excel spreadsheets and aggregated together for input into SmartPLS.

The measurement model was assessed for internal consistency reliability, indicator reliability, convergent validity, and discriminant validity (Hair et al., 2017). The structural model was assessed for collinearity among the constructs, as well as relevance

and significance of the path coefficients (Hair et al., 2017). The results of the SmartPLS analysis with resulting R^2 and path coefficients for the post-workshop survey and data points can be seen in Figure 5.

Figure 5

Post-workshop PLS-SEM Analysis Results



Internal consistency reliability was evaluated with Cronbach's α . Constructs which demonstrated internal consistency reliability by way of Cronbach's α included AH (0.781), CA-RE (0.760), CA-SE (0.915), ISKS (0.663), OB (0.764), and TA-PS (0.913) (Table 20). Like the pre-workshop data analysis, the TA-PV did not meet the cutoff criteria (0.416 versus 0.70). Again, this problem may have been due to the selection of

single questions from three different instruments to develop the questions used in this survey.

Table 20

<i>Post-workshop Cronbach's α (N=42)</i>	
Construct	Cronbach's α
AH	0.781
CA-RE	0.76
CA-SE	0.915
CB	1
ISKS	0.663
OB	0.764
TA-PS	0.913
TA-PV	0.416

Composite reliability of the post-workshop data was assessed with ρ . Levels greater than 0.70 indicated composite reliability for established constructs while values greater than 0.6 are acceptable for exploratory research (Henseler et al., 2016; Wong, 2019). The following constructs indicated composite reliability by virtue of the ρ scores: AC (1.0), AH (0.810), CA-RE (0.795), CA-SE (0.932), CB (1.0), ISKS (0.679), OB (0.801), and TA-PS (0.986) (Table 21). Again, like the pre-workshop analysis, TA-PV did not meet the minimum criteria for ρ . It was theorized that the same situation, having pulled three questions from three different authors surveys may have contributed to this problem.

Table 21

<i>Post-workshop ρ (N=42)</i>	
Construct	ρ
AC	1
AH	0.81
CA-RE	0.795
CA-SE	0.932
CB	1
ISKS	0.679
OB	0.801
TA-PS	0.986
TA-PV	0.55

Convergent validity was assessed using the AVE. The AVE is a grand mean made up of the squared loadings for all the indicators associated with the specific construct (Hair et al., 2017). The AVE from the initial SmartPLS run indicated that the following constructs met AVE requirements (> 0.5): AH (0.505), CA-RE (0.677), CA-SE (0.856), CB (1.0), ISKS (0.602), OB (0.677), and TA-PV (0.849) (Table 22). TA-PV (0.332) was the only construct that did not meet the AVE requirement. This may again be caused by the indicator question selection. The bootstrapped AVE was also calculated for each construct using SmartPLS (Table 23). All constructs were found to have significant AVEs with p-values < 0.001 which indicates that convergent validity was achieved.

Table 22

<i>Post-workshop AVE (N=42)</i>	
Construct	AVE
AH	0.505
CA-RE	0.677
CA-SE	0.856
CB	1
ISKS	0.602
OB	0.677
TA-PS	0.849
TA-PV	0.332

Table 23

Post-workshop Bootstrapped AVE (N=42)

Constructs	Original Sample	<i>M</i>	<i>SD</i>	<i>t</i>	<i>p</i>
AH	0.505	0.541	0.108	4.691	<0.001***
CA-RE	0.677	0.675	0.052	13.132	<0.001***
CA-SE	0.856	0.857	0.041	20.631	<0.001***
ISKS	0.602	0.595	0.07	8.644	<0.001***
OB	0.677	0.681	0.063	10.693	<0.001***
TA-PS	0.849	0.847	0.049	17.156	<0.001***
TA-PV	0.332	0.369	0.065	5.115	<0.001***

* $p < 0.05$; ** $p < 0.01$; *** $p < 0.001$

Discriminant validity was calculated for the post-workshop data to determine if the constructs were conceptually and statistically distinct (Hair et al., 2017). To assess discriminant validity of the reflective measurement models, HTMT was used. Threshold values should be 0.85 (Kline, 2011) or a more liberal cutoff of 0.90 (Gold et al., 2001) can be used. The HTMT values for all constructs met the desired cutoff indicating discriminant validity (Table 24).

Table 24

Post-workshop HTMT (N=42)

Construct	AH	CE-RE	CA-SE	CB	ISKS	OB	TA-PS	TA-PV
AH								
CA-RE	0.181							
CA-SE	0.123	0.707						
CB	0.198	0.207	0.028					
ISKS	0.317	0.789	0.508	0.181				
OB	0.209	0.796	0.64	0.114	0.692			
TA-PS	0.196	0.305	0.18	0.065	0.404	0.35		
TA-PV	0.491	0.564	0.316	0.335	0.372	0.545	0.398	

To analyze the post-workshop structural model, the model was evaluated for collinearity, and the significance and relevance of the latent variable relationships (Hair et

al., 2017). Collinearity was assessed using the VIF (Hair et al., 2017). VIF values were used to determine if a critical level of collinearity has occurred. VIF values below 4.0 indicate that the level of collinearity is acceptable (Hair et al., 2017; Wong, 2019). For the post-workshop structural model all constructs were below the critical value (4.0) (Table 25).

Table 25

Post-workshop VIF (N=42)

Construct	AC	AH	CA-RE	CA-SE	CB	ISKS	OB	TA-PS	TA-PV
AC									
AH								1.059	1.059
CA-RE	3.72								
CA-SE	2.05								
CB			1.012	1.012				1.038	1.038
ISKS		1			1		1		
OB			1.012	1.012				1.039	1.039
TA-PS	1.158								
TA-PV	2.398								

Path coefficients were evaluated to determine their significance and relevance (Hair et al., 2017). Direct effects, indirect effects, and total effects were analyzed. AH has a negative impact on TA-PS (-0.154) and a small positive impact on TA-PV (0.008) (Table 26). CA-RE has a positive impact on AC (0.422). Prior research has demonstrated that CA-RE is related to behavioral intention (Vance et al., 2012). The present research, however, demonstrated that CA-RE was associated with AC behavior. CA-SE had a negative impact on AC (-0.363). This was unexpected since CA-SE has been found to have a positive impact on behavioral intention (Vance et al., 2012). One possible explanation is that the UXAs with high CA-SE feel it is unnecessary to make additional changes to their servers to prevent security breaches. CB has a small negative impact on CA-RE (-0.109). This indicates that as the use of CB increases, the level of CA-RE is

diminished slightly. CB also positively influences TA-PV (0.153), TA-PS (0.121), and CA-SE (0.052). These path coefficients indicate a weak positive relationship between CB and the TA-PV, TA-PS, and CA-SE. ISKS has a strong positive impact on OB (0.697) and a smaller positive influence on AH (0.210). As ISKS increases, OB and AH are positively impacted. ISKS also has a negative impact on CB (-0.172). This indicates that by increasing ISKS there is a negative influence on the use of CB. OB has a positive influence on CA-RE (0.794), CA-SE (0.639), and TA-PS (0.338). As OB increases, CA-RE, CA-SE, and TA-PS increase. OB also has a strong negative impact on TA-PV (-0.751). This indicates that as OB increases the TA-PV decreases. TA-PS and TA-PV have a negative impact on AC (-0.196 and -0.128 respectively).

Table 26

Post-workshop Path Coefficients (N=42)

Construct	AC	AH	CA-RE	CA-SE	CB	ISKS	OB	TA-PS	TA-PV
AC									
AH								-0.154	0.008
CA-RE	0.422								
CA-SE	-0.363								
CB			-0.109	0.052				0.121	0.153
ISKS		0.21			-0.172		0.697		
OB			0.794	0.639				0.338	-0.751
TA-PS	-0.196								
TA-PV	-0.128								

Total indirect effects were evaluated to assess the impact of interim constructs. Notably, ISKS had positive impacts on CA-RE (0.572), CA-SE (0.436), TA-PS (0.182), and AC (0.117) (Table 27). This indicated that as ISKS increases CA-RE, CA-SE, TA-PS, and AC behavior increase. ISKS also had a strong negative impact on TA-PV (-0.548). Given that additional knowledge may afford the UXA new skills needed to protect their servers, reducing TA-PV may be a reasonable response to the training. AH was

determined to have a small positive indirect effect on AC (0.029). This may be due to slightly larger indirect specific effect AH->TA-PS->AC (0.030) versus the smaller negative indirect effect AH->TA-PV->AC (-0.001). CB was found to have a small negative impact on AC (-0.108). This value is very low and indicated the weak influence that the bias may have on compliance behavior. This may be due to the accumulation of slight specific indirect effects CB->CA-RE->AC (-0.046), CB->CA-SE->AC (-0.019), CB->TA-PS->AC (-0.024), and CB->TA-PV->AC (-0.02). Finally, OB was reported to have a small positive influence on AC (0.133). It is interesting that, as the use of OB increases there is a small increase in AC.

Table 27

<i>Post-workshop Indirect Effects (N=42)</i>									
Construct	AC	AH	CA-RE	CA-SE	CB	ISKS	OB	TA-PS	TA-PV
AC									
AH	0.029								
CA-RE									
CA-SE									
CB	-0.108								
ISKS	0.117		0.572	0.436				0.182	-0.548
OB	0.133								
TA-PS									
TA-PV									

The most significant positive specific indirect effects included ISKS->OB->CA-RE (0.554), ISKS->OB->CA-SE (0.445), OB->CA-RE->AC (0.335), ISKS->OB->TA-PS (0.236), and ISKS->OB->CA-RE->AC (0.233) (Table 28). The most significant negative specific indirect effects included ISKS->OB->TA-PV (-0.524), OB->CA-SE->AC (-0.232), and ISKS->OB->CA-SE->AC (-0.162).

Table 28

<i>Post-workshop Specific Indirect Effects (N=42)</i>	
Path	Specific Indirect Effects
CB->CA-RE->AC	-0.046
ISKS->CB->CA-RE->AC	0.008
OB->CA-RE->AC	0.335
ISKS->OB->CA-RE->AC	0.233
CB->CA-SE->AC	-0.019
ISKS->CB->CA-SE->AC	0.003
OB->CA-SE->AC	-0.232
ISKS->OB->CA-SE->AC	-0.162
AH->TA-PS->AC	0.03
ISKS->AH->TA-PS->AC	0.006
CB->TA-PS->AC	-0.024
ISKS->CB->TA-PS->AC	0.004
OB->TA-PS->AC	-0.066
ISKS->OB->TA-PS->AC	-0.046
AH->TA-PV->AC	-0.001
ISKS->AH->TA-PV->AC	0
CB->TA-PV->AC	-0.02
ISKS->CB->TA-PV->AC	0.003
OB->TA-PV->AC	0.096
ISKS->OB->TA-PV->AC	0.067
ISKS->CB->CA-RE	0.019
ISKS->OB->CA-RE	0.554
ISKS->CB->CA-SE	-0.009
ISKS->OB->CA-SE	0.445
ISKS->AH->TA-PS	-0.032
ISKS->CB->TA-PS	-0.021
ISKS->OB->TA-PS	0.236
ISKS->AH->TA-PV	0.002
ISKS->CB->TA-PV	-0.026
ISKS->OB->TA-PV	-0.524

Due to the presence of mediating latent variables, the total effects must be computed. Total effects were computed using SmartPLS (Table 29). AH had a small positive influence on AC (0.029) and TA-PV (0.008). Also, AH had a small negative influence on TA-PS (-0.154). CA-RE had a moderate impact on AC (0.422). This result was consistent with prior research that found that CA-RE predicted behavioral intention

(Vance et al., 2012). CA-SE had a moderate negative effect on AC (-0.363). This result was puzzling as prior research had found that CA-SE was associated with compliance intention (Safa et al., 2015; Vance et al., 2012). CB had small negative effects on AC (-0.108) and CA-RE (-0.109). This seems logical since the use of this bias negatively impacts compliance and CA-RE. CB had a positive effect on CA-SE (0.052), TA-PS (0.121), and TA-PV (0.153). ISKS had strong positive effect on OB (0.697), CA-RE (0.572), CA-SE (0.436). ISKS had a weak positive effect on AH (0.210), TA-PS (0.182), and AC (0.117). This indicated that knowledge sharing improved TA-PS and AC. ISKS had a strong negative effect on TA-PV (-0.751) and a weak negative effect on CB (-0.172). The benefit of ISKS, in terms of CA-RE and CA-SE, is in line with prior research (Vance et al., 2012). The negative influence of ISKS on the use of CB demonstrates the value of training in reducing the use of CB. The significant negative effect of ISKS on TA-PV (-0.548) indicated that the knowledge sharing helped to reduce the vulnerability the UXAs perceived. Clearly, in this situation, knowledge was power. OB had a strong positive effect on CA-RE (0.794) and CA-SE (0.639). Additionally, OB had a moderate positive effect on TA-PS (0.338) and a weak positive effect on AC (0.133). Given that OB tends to make one feel invulnerable it is logical that the CA-RE and CA-SE are positively related.

Table 29

Post-workshop Total Effects (N=42)

Construct	AC	AH	CA-RE	CA-SE	CB	ISKS	OB	TA-PS	TA-PV
AC									
AH	0.029							-0.154	0.008
CA-RE	0.422								
CA-SE	-0.363								
CB	-0.108		-0.109	0.052				0.121	0.153
ISKS	0.117	0.21	0.572	0.436	-0.172		0.697	0.182	-0.548
OB	0.133		0.794	0.639				0.338	-0.751
TA-PS	-0.196								
TA-PV	-0.128								

The significance of the path coefficients was evaluated using bootstrapping in SmartPLS. This technique, in SmartPLS, generates T-statistics for both outer and inner models (Wong, 2019). The paths that had significant p-values included ISKS->OB (<0.001), OB->CA-RE (<0.001), OB->CA-SE (<0.001), and OB->TA-PS (0.017) (Table 30). Based on these results it was reasonable to conclude that the workshop had a significant influence on the use of OB and that OB significantly influenced RE, SE, and PS.

Table 30

Post-workshop Bootstrapped Path Coefficients (N=42)

Path	Original Sample	M	SD	t	p
ISKS->OB	0.511	0.521	0.141	3.631	<0.001***
OB->CA-RE	0.638	0.647	0.103	6.197	<0.001***
OB->CA-SE	0.549	0.548	0.119	4.626	<0.001***
OB->TA-PS	0.326	0.309	0.154	2.12	0.017*

* p < 0.05; ** p < 0.01; *** p < 0.001

The effect size (f^2) was evaluated to determine how one construct contributed to the explaining power of other constructs (Hair et al., 2017; Wong, 2019). The effect sizes

were computed using SmartPLS (Table 31). Strong positive effects included OB->CA-RE (1.839), OB->TA-PV (1.412), ISKS->OB (0.945), and OB->CA-SE (0.675). Clearly, OB was a significant influencer in the model. Weak positive effects included OB->TA-PS (0.130), CA-SE->AC (0.076), CA-RE->AC (0.056), AH->TA-PS (0.027), CB->CA-RE (0.035), CB->TA-PV (0.059), ISKS->AH (0.046), ISKS->CB (0.031), and TA-PS->AC (0.039).

Table 31

<i>Post-workshop Effect Size (N=42)</i>									
Construct	AC	AH	CA-RE	CA-SE	CB	ISKS	OB	TA-PS	TA-PV
AC									
AH								0.027	0.000
CA-RE	0.056								
CA-SE	0.076								
CB			0.035	0.004				0.017	0.059
ISKS		0.046			0.031		0.945		
OB			1.839	0.675				0.13	1.412
TA-PS	0.039								
TA-PV	0.008								

Blindfolding was used to test predictive relevance using the Stone-Geisser values (Wong, 2019). Constructs with significant predictive power are indicated in Table 32. Constructs found to provide moderate predictive power included CA-RE (0.265), CA-SE (0.231), and OB (0.164). TA-PS (0.044) was found to have weak predictive power in the post-workshop model.

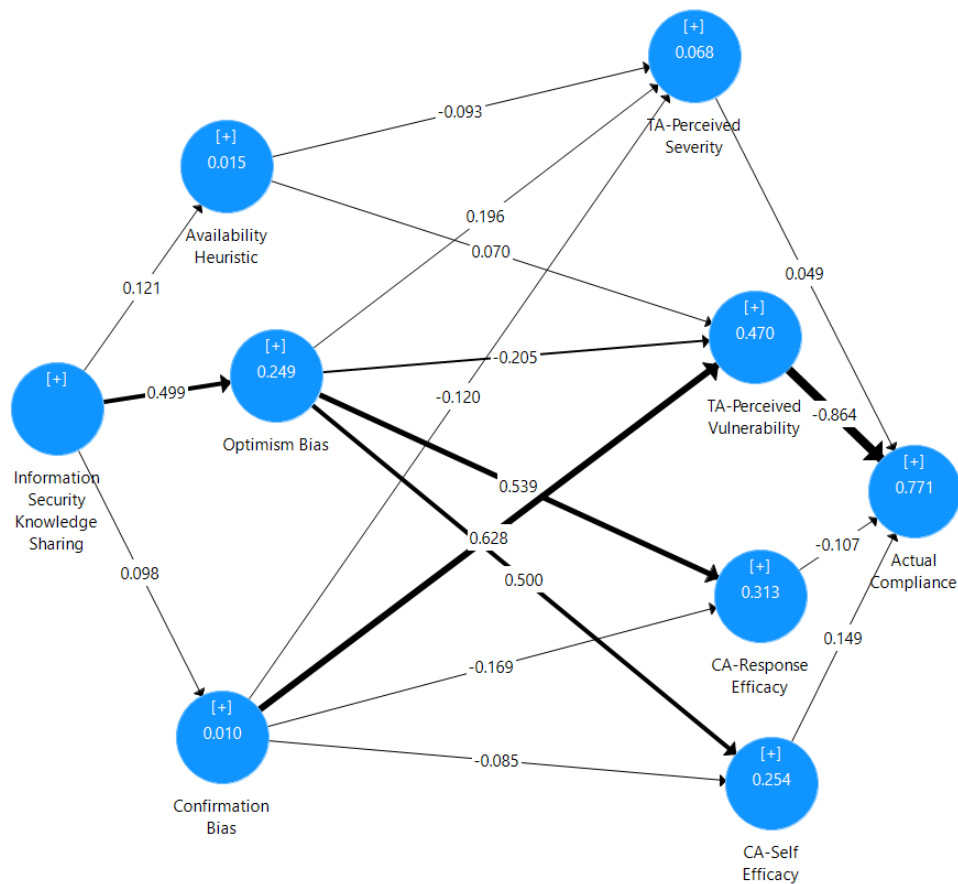
Table 32

<i>Post-workshop Predictive Power (N=42)</i>		
Construct	Q ²	Predictive Power
CA-RE	0.265	Moderate
CA-SE	0.231	Moderate
OB	0.164	Moderate
TA-PS	0.044	Weak

The next step in the analysis of the data was to perform SmartPLS Multigroup Analysis (PLS-MGA). Both datasets were merged, and a group identifier column was added to differentiate before-workshop and after-workshop data. The same model was used for the multigroup analysis. The measurement model was assessed for internal consistency reliability, indicator reliability, convergent validity, and discriminant validity (Hair et al., 2017). The structural model was assessed for collinearity among the constructs, as well as relevance and significance of the path coefficients (Hair et al., 2017). The combined groups model with R^2 and path coefficients can be found in Figure 6.

Figure 6

Combined Groups PLS-SEM Analysis Results



Internal consistency reliability for the multigroup model was evaluated with Cronbach's α . Constructs which demonstrated internal consistency reliability by way of Cronbach's α include AH (0.631), CA-RE (0.711), CA-SE (0.881), ISKS (0.675), OB (0.731), and TA-PS (0.883) (Table 33). Like both the pre-workshop and post-workshop data analysis, the TA-PV did not meet the cutoff criteria (0.444 versus 0.70).

Table 33

Multigroup Cronbach's α (N=84)

Construct	Cronbach's α
AH	0.631
CA-RE	0.711
CA-SE	0.881
CB	1
ISKS	0.675
OB	0.731
TA-PS	0.883
TA-PV	0.444

Composite reliability of the post-workshop data were assessed with ρ . The following constructs indicated composite reliability by virtue of the ρ scores AC (1.0), AH (0.819), CA-RE (0.758), CA-SE (0.882), CB (1.0), ISKS (0.756), OB (0.775), and TA-PS (0.924) (Table 34). Again, like the pre-workshop and post-workshop analyses, TA-PV did not meet the minimum criteria for ρ .

Table 34

<i>Multigroup ρ (N=84)</i>	
Construct	ρ
AC	1
AH	0.819
CA-RE	0.758
CA-SE	0.882
CB	1
ISKS	0.756
OB	0.775
TA-PS	0.924
TA-PV	0.328

Convergent validity of the multigroup model was assessed using the AVE.

Constructs that met the cutoff for AVE included AH (0.506), CA-RE (0.632), CA-SE (0.807), ISKS (0.596), OB (0.649), and TA-PS (0.805) (Table 35). TA-PV did not meet the cutoff for AVE potentially due to the use of individual questions from three different surveys. The bootstrapped AVE was also calculated for each construct using SmartPLS (Table 36). All constructs were found to have significant AVEs with p-values < 0.001 which indicates that convergent validity was achieved.

Table 35

<i>Multigroup AVE (N=84)</i>	
Construct	AVE
AH	0.506
CA-RE	0.632
CA-SE	0.807
ISKS	0.596
OB	0.649
TA-PS	0.805
TA-PV	0.26

Table 36*Multigroup Bootstrapped AVE (N=84)*

Construct	Original Sample	<i>M</i>	<i>SD</i>	<i>t</i>	<i>p</i>
AH	0.506	0.495	0.056	9.071	<0.001***
CA-RE	0.632	0.628	0.052	12.191	<0.001***
CA-SE	0.807	0.808	0.045	17.759	<0.001***
ISKS	0.596	0.59	0.059	10.126	<0.001***
OB	0.649	0.647	0.043	14.919	<0.001***
TA-PS	0.805	0.783	0.105	7.636	<0.001***
TA-PV	0.26	0.296	0.036	7.143	<0.001***

* $p < 0.05$; ** $p < 0.01$; *** $p < 0.001$

Discriminant validity was calculated for the multigroup data to determine if the constructs were conceptually and statistically distinct (Hair et al., 2017). To assess discriminant validity of the reflective measurement models, HTMT was used. The HTMT values for all constructs met the desired cutoff indicating discriminant validity (Table 37).

Table 37*Multigroup HTMT (N=84)*

Construct	AH	CA-RE	CA-SE	CB	ISKS	OB	TA-PS	TA-PV
AH								
CA-RE	0.261							
SA-SE	0.269	0.776						
CB	0.515	0.191	0.106					
ISKS	0.33	0.768	0.621	0.143				
OB	0.222	0.676	0.608	0.109	0.654			
TA-PS	0.212	0.386	0.174	0.153	0.387	0.226		
TA-PV	0.58	0.315	0.228	0.542	0.228	0.357	0.348	

To analyze the multigroup structural model, the model was evaluated for collinearity, as well as the significance and relevance of the relationships (Hair et al., 2017). Collinearity was assessed using the VIF (Hair et al., 2017). For the post-workshop structural model all constructs were below the critical value (4.0) (Table 38).

Table 38

Multigroup VIF (N=84)

Construct	AC	AH	CA-RE	CA-SE	CB	ISKS	OB	TA-PS	TA-PV
AC									
AH								1.237	1.237
CA-RE	1.782								
CA-SE	1.645								
CB			1.001	1.001				1.238	1.238
ISKS		1			1		1		
OB			1.001	1.001				1.002	1.002
TA-PS	1.112								
TA-PV	1.038								

Path coefficients were of the multigroup model were evaluated to determine their significance and relevance (Hair et al., 2017). The most significant influencer of AC was TA-PV (-0.864) (Table 39). CA-SE had a positive impact on AC (0.149). CB had a positive impact on TA-PV (0.628). As ISKS and security updates increased awareness and it seems logical that it would increase the perceived vulnerabilities facing the UXAs. ISKS had a weak positive impact on AH (0.121), CB (0.098), and a strong positive influence on OB (0.499). OB had a weak positive impact on TA-PS (0.196), CA-SE (0.500), and CA-RE (0.539). Again, training and education may have increased the UXAs' optimism about their ability to protect their servers. This would be reflected in increased CA-RE, CA-SE, and TA-PS. The negative influence of OB on TA-PV (-0.205) may indicate that the workshop and security emails increased awareness of the vulnerabilities facing the UXAs. TA-PS had a weak positive influence on AC (0.049).

Table 39*Multigroup Path Coefficients (N=84)*

Construct	AC	AH	CA-RE	CA-SE	CB	ISKS	OB	TA-PS	TA-PV
AC									
AH								-0.093	0.07
CA-RE	-0.107								
CA-SE	0.149								
CB			-0.169	-0.085				-0.12	0.628
ISKS		0.121			0.098		0.499		
OB			0.539	0.5				0.196	-0.205
TA-PS	0.049								
TA-PV	-0.864								

Total indirect effects were evaluated to assess the impact of interim constructs (Table 40). AH had a weak negative influence on AC (-0.065). This weak influence may be due to the increased knowledge of the significant vulnerabilities facing the UXAs and their perception of impotence in mitigating the risks. CB had a strong negative impact on AC (-0.543). It is logical that an increased use of CB has a substantial negative impact on compliance behavior. ISKS had a weak positive influence on AC (0.040), TA-PS (0.074), and a moderate influence on CA-RE (0.252), and CA-SE (0.241). The workshop and security updates increased awareness and increased the UXAs compliance, and belief that they can respond effectively to the risks. ISKS did have a weak negative influence on TA-PV (-0.032). As noted previously, this reduced TA-PV may be due to the UXAs being introduced to tools and actions they can do to reduce the vulnerabilities facing their servers. Finally, OB had a moderately positive influence on AC (0.204). UXAs optimism related to IS risk seemed to encourage compliance behavior.

Table 40*Multigroup Indirect Effect (N=84)*

Construct	AC	AH	CA-RE	CA-SE	CB	ISKS	OB	TA-PS	TA-PV
AC									
AH	-0.065								
CA-RE									
CA-SE									
CB	-0.543								
ISKS	0.04		0.252	0.241				0.074	-0.032
OB	0.204								
TA-PS									
TA-PV									

The most significant positive specific indirect effects included ISKS->OB->CA-RE (0.269), and OB->TA-PV->AC (0.177) (Table 41). The most significant negative specific indirect effects included CB->TA-PV->AC (-0.543), ISKS->OB->CA-SE (-0.249), ISKS->OB->TA-PV (-0.102).

Table 41

<i>Multigroup Specific Indirect Effect (N=84)</i>	
Path	Specific Indirect Effects
CB->CA-RE->AC	0.018
ISKS->CB->CA-RE->AC	0.002
OB->CA-RE->AC	-0.058
ISKS->OB->CA-RE->AC	-0.029
CB->CA-SE->AC	-0.013
ISKS->CB->CA-SE->AC	-0.001
OB->CA-SE->AC	0.074
ISKS->OB->CA-SE->AC	0.037
AH->TA-PS->AC	-0.005
ISKS->AH->TA-PS->AC	-0.001
CB->TA-PS->AC	-0.006
ISKS->CB->TA-PS->AC	-0.001
OB->TA-PS->AC	0.01
ISKS->OB->TA-PS->AC	0.005
AH->TA-PV->AC	-0.061
ISKS->AH->TA-PV->AC	-0.007
CB->TA-PV->AC	-0.543
ISKS->CB->TA-PV->AC	-0.053
OB->TA-PV->AC	0.177
ISKS->OB->TA-PV->AC	0.088
ISKS->CB->CA-SE	-0.017
ISKS->OB->CA-RE	0.269
ISKS->CB->CA-SE	-0.008
ISKS->OB->CA-SE	0.249
ISKS->AH->TA-PS	-0.011
ISKS->CB->TA-PS	-0.012
ISKS->OB->TA-PS	0.098
ISKS->AH->TA-PV	0.009
ISKS->CB->TA-PV	0.062
ISKS->OB->TA-PV	-0.102

Due to the presence of mediating latent variables, the total effects were computed.

Total effects for the multigroup model were computed using SmartPLS (Table 42). AH had a weak negative total effect on AC (-0.065) and TA-PS (-0.093) as well as a weak positive total effect on TA-PV (0.070). These minor effects may be due to increased availability of IS risk and vulnerabilities presented by the workshop and security update

emails. CA-RE had a negative influence on AC (-0.107). This is contrary to other research that found CA-RE to be a positive influencer of behavioral intention (Vance et al., 2012). UXAs may, in believing their response effectiveness is high, decided there was no need to implement suggested security changes. CA-SE had a positive impact on ACH (0.149). This is in line with prior research on CA-SE and behavioral intention (Safa et al., 2016; Vance et al., 2012). CB had a strong negative influence on AC (-0.543), a moderate negative influence on CA-RE (-0.169), and weak negative impact on CA-SE (-0.085), and TA-PS (-0.120). Logically, as CB increases, there may be increased resistance to the implementation of security controls and guidelines. The moderate and weak negative influences on CA-RE, and CA-SE imply that the bias may reduce the UXAs belief in their ability to respond to IS risks. The negative influence of CB on TA-PS (-0.120) indicates that as UXAs increase their use of this bias it has a negative effect on their TA-PS of an IS breach. Last, the positive impact of CB on TA-PV (0.628) indicated that the increased use of this bias may lead to increased levels of TA-PV. ISKS had a strong positive influence on OB (0.499), moderate positive influence on CA-RE (0.252), CA-SE (0.241), and weak positive influence on AH (0.121), TA-PS (0.074), and AC (0.040). ISKS had a weak negative impact on TA-PV (-0.032). Each of these findings, for the established constructs, were in line with prior research on ISKS (Posey et al., 2015). The positive effect of ISKS on OB, AH, and CB demonstrated that the workshop and security updates did have an impact on the participants. The strong influence of ISKS on OB may indicate, based on the questions, that they perceive themselves as more resilient and able to cope with the IS risks facing them. OB had strong positive total effects on CA-RE (0.539), CA-SE (0.500), and moderate positive total effects on AC (0.204), and TA-PS

(0.196). Finally, OB had a moderate negative effect on TA-PV (-0.205). It seemed logical that increased optimistic bias resulted in increased CA-RE and CA-SE for the UX. The positive impact of OB on AC and TA-PS indicated that the increased use of the bias did ultimately result in increased behavioral compliance. Lastly, the negative relationship between OB and TA-PV indicated that the increased use of this bias may lead to reduced TA-PV. TA-PS had a weak positive effect on AC (0.049). This finding is in line with prior research that tied TA-PS to behavioral intention (Bélanger et al., 2017; Posey et al., 2015; Siponen et al., 2014). Finally, TA-PV had a strong negative effect on AC (-0.864).

Table 42

Multigroup Total Effects (N=84)

Construct	AC	AH	CA-RE	CA-SE	CB	ISKS	OB	TA-PS	TA-PV
AC									
AH	-0.065							-0.093	0.07
CA-RE	-0.107								
CA-SE	0.149								
CB	-0.543		-0.169	-0.085				-0.12	0.628
ISKS	0.04	0.121	0.252	0.241	0.098		0.499	0.074	-0.032
OB	0.204		0.539	0.5				0.196	-0.205
TA-PS	0.049								
TA-PV	-0.864								

The significance of the path coefficients for the multigroup were evaluated using bootstrapping in SmartPLS (Table 43). The paths that had significant p-values included CB->TA-PV (<0.001), ISKS->OB (<0.001), OB->CA-RE (<0.001), OB->CA-SE (<0.001), OB->CA-SE (<0.001), OB->TA-PS (0.047), OB->TA-PV (0.022), and TA-PV->AC (<0.001). These results indicated that ISKS and OB had significant impact on the PMT constructs and ultimately AC behavior.

Table 43*Multigroup Bootstrapped Path Coefficients (N=84)*

Path	Original Sample	M	SD	t	p
AH->TA-PS	-0.093	-0.082	0.146	0.634	0.263
AH->TA-PV	0.07	0.082	0.107	0.661	0.254
CA-RE->AC	-0.107	-0.1	0.087	1.235	0.108
CA-SE->AC	0.149	0.152	0.096	1.542	0.062
CB->CA-RE	-0.169	-0.167	0.122	1.378	0.084
CB->CA-SE	-0.085	-0.085	0.12	0.702	0.241
CB->TA-PS	-0.12	-0.099	0.154	0.78	0.218
CB->TA-PV	0.628	0.606	0.121	5.197	<0.001***
ISKS->AH	0.121	0.119	0.158	0.769	0.221
ISKS->CB	0.098	0.094	0.113	0.867	0.193
ISKS->OB	0.499	0.509	0.085	5.834	<0.001***
OB->CA-RE	0.539	0.545	0.081	6.647	<0.001***
OB->CA-SE	0.5	0.507	0.072	6.956	<0.001***
OB->TA-PS	0.196	0.187	0.117	1.678	0.047*
OB->TA-PV	-0.205	-0.201	0.102	2.006	0.022*
TA-PS->AC	0.049	0.028	0.082	0.592	0.277
TA-PV->AC	-0.864	-0.843	0.117	7.394	<0.001***

* p < 0.05; ** p < 0.01; *** p < 0.001

The effect size (f^2) was evaluated to determine how one construct contributed to the explaining power of other constructs (Hair et al., 2017; Wong, 2019). Strong positive effects included TA-PV->AC (3.142), CB->TA-PV (0.602) (Table 44). Moderate positive effects included: OB->CA-RE (0.423), OB->CA-SE (0.334), and ISKS->OB (0.331). Weak positive effects included OB->TA-PV (0.079), CA-SE->AC (0.059), CB->CA-RE (0.041), OB->TA-PS (0.041), and CA-RE->AC (0.028).

Table 44*Multigroup Effect Size (N=84)*

Construct	AC	AH	CA-RE	CA-SE	CB	ISKS	OB	TA-PS	TA-PV
AC									
AH								0.007	0.008
CA-RE	0.028								
CA-SE	0.059								
CB			0.041	0.010				0.013	0.602
ISKS		0.015			0.010		0.331		
OB			0.423	0.334				0.041	0.079
TA-PS	0.009								
TA-PV	3.142								

Blindfolding was used to test predictive relevance using the Stone-Geisser values (Wong, 2019). AC (0.352) had strong predictive power in the model (Table 45). CA-SE (0.185) had moderate predictive power. OB (0.146) and TA-PV (0.086) had weak predictive power in the multigroup model.

Table 45*Multigroup Predictive Power (N=84)*

Construct	Q ²	Predictive Power
AC	0.352	Strong
AH	0.002	
CA-RE	0.149	Weak
CA-SE	0.185	Moderate
CB	-0.006	
OB	0.146	Weak
TA-PS	0.016	
TA-PV	0.086	Weak

Descriptive Statistic Analysis

To assess changes in the use of AH, OB, and CB, the pre- and post-data for each variable were aggregated and t-statistics were computed for each. For AH, the four variables pre-workshop and post-workshop were compared with paired t-tests. For OB,

the three variables pre-workshop and post-workshop were compared with paired t-tests. Finally, for CB, the single variable was compared pre-workshop and post-workshop with a paired T-Test. This process allowed for a single paired t-test to be performed for each latent variable. The results (Table 46) indicated that AH ($t=3.914$, $p<0.001$) and CB ($t=7.723$, $p<0.001$) had a significant change from before the workshop to after the workshop. The mean for AH went from 4.667 to 4.155 indicating that the AH was not as impactful post-workshop. Similarly, the CB mean changed from 2.095 to 0.333 which indicated a significant reduction in the use of CB. OB, however, did not show a significant change from pre-workshop to post-workshop ($t=-2.353$, $p=0.010$). Figure 7 provides a graphical representation of the before intervention and after intervention means for the three cognitive heuristics and biases constructs.

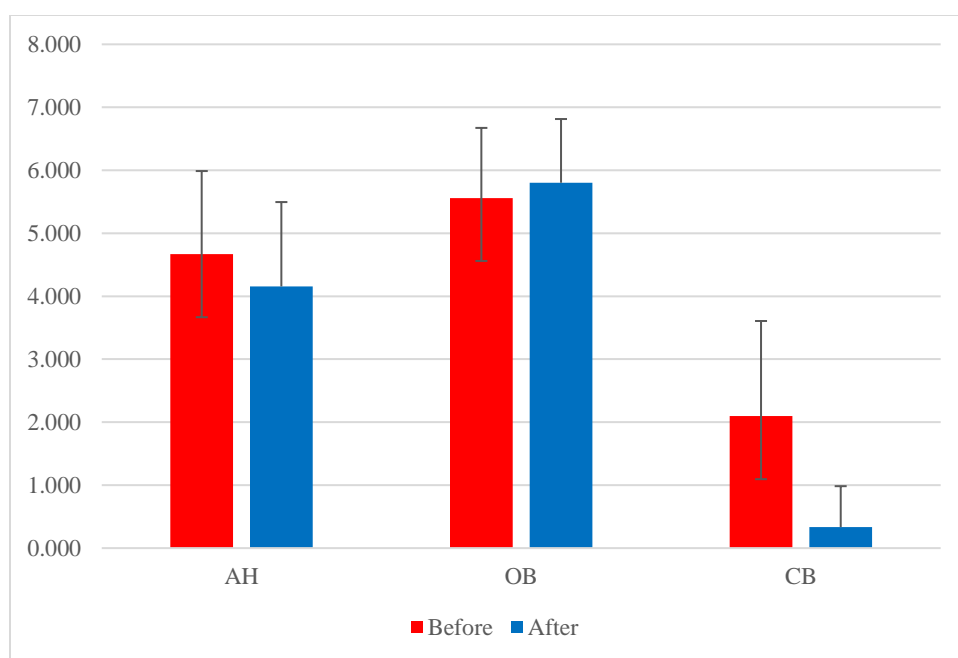
Table 46

<i>Cognitive Heuristics and Biases Descriptive Statistics</i>			
	AH (N=168)	OB (N=126)	CB (N=42)
Before Mean	4.667	5.56	2.095
Before Variance	1.745	1.238	2.283
After Mean	4.155	5.802	0.333
After Variance	1.796	1.024	0.423
Observations	168	126	42
Pearson Correlation	0.188	0.415	0.265
Hypothesized Mean Difference	0	0	0
df	167	125	41
t	3.914	-2.353	7.723
P(T<=t) one-tail	<0.001***	0.01*	<0.001***
t Critical one-tail	1.654	1.657	1.683

* $p < 0.05$; ** $p < 0.01$; *** $p < 0.001$

Figure 7

Cognitive heuristics and biases with M and σ

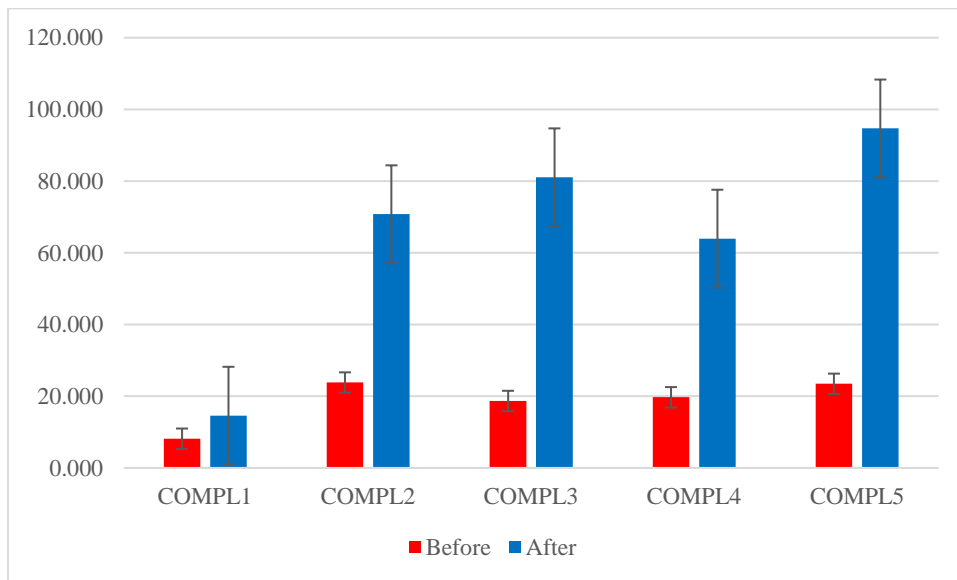


Finally, to assess the changes in AC behavior, paired t-tests were run on all pre- and post-workshop compliance indicators (Table 47). All five compliance indicators demonstrated significant change from pre- to post-workshop. It was interesting to note that the most frequently implemented security changes were ones that the UXA had complete control over including the following: server patching, local firewall implementation, and MFA implementation. The two lowest scoring behavioral changes were for security changes that required interfacing with the organization's IS team (Tenable Nessus and Splunk implementations). Figure 8 provides a graphical representation of the means for each of the compliance indicators before and after the workshop.

Table 47*Compliance T-Test Results (N=42)*

	COMPL1	COMPL2	COMPL3	COMPL4	COMPL5
Before Mean	8.149	23.817	18.668	19.708	23.462
After Mean	14.575	70.770	81.081	63.961	94.697
Before Variance	419.159	1410.759	678.934	536.833	489.736
After Variance	722.818	1346.618	867.276	1610.410	123.446
Pearson Correlation	0.824	0.423	0.239	0.462	-0.250
df	41	41	41	41	41
<i>t</i>	2.721	7.625	11.779	7.989	17.014
<i>P</i> (T<=t) one-tail	0.005**	<0.001***	<0.001***	<0.001***	<0.001***
<i>t</i> Critical one-tail	1.683	1.683	1.683	1.683	1.683

* $p < 0.05$; ** $p < 0.01$; *** $p < 0.001$

Figure 8*Compliance metrics with M and SE***Findings**

For hypotheses H1-3, the paired t-statistics were used to assess significance. To test hypotheses H4a-H8b the data from the PLS-MGA multigroup bootstrapped path analysis results were used to assess path significance. Hypotheses that were accepted were H1, H3, H5a, H5b, H5c, H5d, H6b, and H7b (Table 48). H2, H4a, H4b, H6a, H6c,

H6d, H7a, H8a, and H8b were rejected. These results indicated that the workshop, ISC, and security update emails did have a significant impact on the use of AH, and CB but not OB.

Table 48

Hypotheses responses

Hypothesis	<i>t</i>	<i>p</i>	Accept/Reject
H1: ISKS -> AH	3.914	<0.001***	Accepted
H2: ISKS -> OB	-2.353	0.01	Rejected
H3: ISKS -> CB	7.723	<0.001***	Accepted
H4a: AH -> TA-PS	0.634	0.263	Rejected
H4b: AH -> TA-PV	0.661	0.254	Rejected
H5a: OB -> TA-PS	1.678	0.047*	Accepted
H5b: OB -> TA-PV	2.006	0.022*	Accepted
H5c: OB -> CA-SE	6.956	<0.001***	Accepted
H5d: OB -> CA-RE	6.647	<0.001***	Accepted
H6a: CB -> TA-PS	0.78	0.218	Rejected
H6b: CB -> TA-PV	2.006	<0.001***	Accepted
H6c: CB -> CA-SE	0.702	0.241	Rejected
H6d: CB -> CA-RE	1.378	0.084	Rejected
H7a: TA-PS -> AC	0.592	0.277	Rejected
H7b: TA-PV -> AC	7.394	<0.001***	Accepted
H8a: CA-RE -> AC	1.235	0.108	Rejected
H8b: CA-SE -> AC	1.542	0.062	Rejected

* $p < 0.05$; ** $p < 0.01$; *** $p < 0.001$

Summary

The goal was to empirically assess the effect of a focused SETA workshop, an ISC, and periodic security update emails on UXAs' knowledge sharing, use of cognitive heuristics, biases, threat appraisal, coping appraisal, and ISP compliance behavior. To accomplish this, participants completed a survey prior to the intervention. Additionally, AC behavior data points were collected from script, Tenable Nessus, Splunk, and organizational databases. The pre-workshop data were evaluated using SmartPLS to assess the reliability and validity of the indicators and constructs, as well as the

significance of path coefficients in the model. Ninety days following the workshop, ISC, and security emails, participants completed a post-workshop survey, and AC data points were collected again. This post-workshop data were evaluated in SmartPLS. Following those two analyses, a multigroup analysis was completed using the merged before and after data. This analysis provided the significant path coefficients that were used to answer hypotheses H4a-H8b. T-Tests were used to evaluate changes in AC, OB, and CB to answer H1-H3. Based on these analyses, eight hypotheses were accepted, and nine hypotheses were rejected.

Chapter 5

Conclusions, Implications, Recommendations, and Summary

Overview

This chapter includes conclusions that were drawn from the data analysis followed by a discussion about the study's limitations, strengths, and weaknesses. Next, implications of this research on organizational security training are discussed. Finally, recommendations for future research are identified. This chapter closes with a concise summary of the study.

Conclusions

The goal was to empirically assess the effect of a focused SETA workshop, an ISC, and periodic security update emails on UXAs' knowledge sharing, use of cognitive heuristics, biases, threat appraisal, coping appraisal, and ISP compliance behavior. Based on the t-statistical analysis, the use of AH and CB were significantly influenced by the security workshop, ISC, and security update emails. This finding is encouraging as it implied that changes in IS behavior can be accomplished through IS training. Unfortunately, OB did not meet the statistical cutoff for significance. It did, however, have a statistically significant influence on TA-PS, TA-PV, CA-SE, and CA-RE. It is possible that a larger sample size might have increased the significance and demonstrated how OB was influenced by ISKS. Based on the PLS multigroup analysis, OB and CB did have significant effects on TA-PS, TA-PV, CA-SE, and CA-RE.

In the post-group analysis, CA-SE had a negative impact on AC (-0.363). This was unexpected since CA-SE has been found to have a positive impact on behavioral

intention (Vance et al., 2012). One possible explanation is that the UXAs with high CA-SE feel it was unnecessary to make additional changes to their servers to prevent security breaches. Also, in the post-group analysis, TA-PS and TA-PV had a negative impact on AC (-0.196 and -0.128 respectively). While these values are not very strong it is curious to note that increased TA-PS or TA-PV resulted in reduced compliance. It was possible that this was due to the increased awareness of the potential problems that the UXAs must mitigate resulting in a sense of being overwhelmed and throwing up their hands in defeat. Also, in the post-group analysis, it was interesting that, as the use of OB increases there is a small increase in AC. This may be due to the substantial specific indirect effect (0.335) from OB->CA-RE->AC. The negative relationship of OB and TA-PV (0.751) seems appropriate since OB makes one feel invulnerable. The positive effect of OB on TA-PS (0.338) may be due to UXAs feeling optimistic regarding the possibility their servers may be breached but still understanding that a breach would be severe for the organization and the individual.

In the multigroup analysis, the most significant influencer of AC was TA-PV (-0.864). Two considerations that may have resulted in this strongly negative relationship. First, the UXAs may have been overwhelmed by the vulnerabilities facing them which could result in a failure to implement security measures. Another consideration could be problems associated with the survey questions used. As noted earlier, Cronbach's α and ρ were below statistical requirements for the four TA-PV questions. AH had a small negative influence on TA-PS (-0.093) and a small positive influence on TA-PV (0.070). CA-RE had a negative influence on AC (-0.107). This is contrary to other research which found that CA-RE was a positive influence on compliance intention (Siponen et al., 2014,

Vance et al., 2012). CA-SE had a positive impact on AC (0.149). This is in line with prior research where individual CA-SE was positive related to compliance intention (Safa et al., 2016; Siponen et al., 2014, Vance et al., 2012). CB had a negative influence on CA-RE (-0.169), CA-SE (-0.085), and TA-PS (-0.120). This may be due to the education and alerts challenging the CB and resulting in reduced CA-RE, CA-SE, and TA-PS. ISKS had a weak positive impact on AH (0.121), CB (0.098), and a strong positive influence on OB (0.499). The workshop and security updates may have increased participant's alertness to vulnerability reports in the news which may have resulted in increased availability of incidents. The strong positive impact of ISKS on OB may indicate that the education raised awareness of tools and methods of securing their servers. This is a positive change as it indicates that the education does help UXAs increase awareness and improve the security of their servers. TA-PS had a weak positive influence on AC (0.049). It seems logical that increased TA-PS of the impact of a breach would positively influence compliance behavior. TA-PV had a strong negative impact on AC (-0.864). As mentioned earlier, this may be due to a sense of being overwhelmed by the number of vulnerabilities and risks facing the UXAs and their deciding that they unable to make the changes needed. This result may also be due to the problems related to the survey questions for TA-PV. Finally, for the multigroup analysis, TA-PV had a strong negative effect on AC (-0.864). This may be attributed to the problems associated with the questions previously mentioned, it may be the result of UXAs being overwhelmed by the work facing them, or it could be related to the independent, free-thinking nature of UXAs in resisting control by the organization (Markowitz, 2016).

One strength of this study was the use of AC metrics rather than relying on

reported behavioral intention. These metrics allowed for an assessment of actual security changes made by the UXAs following the workshop, ISC, and security update emails. It was encouraging that all the behavioral metrics analyzed showed significant change between pre-workshop and post-workshop analysis. COMPL3 (local firewall) and COMPL5 (patching) had the highest degree of change based on the t-statistics.

Interestingly, these two actions were actions the UXA could take on their own with no interaction with the IS team. COMPL2 (Tenable) and COMPL4 (MFA) required minor interaction with the IS team in that the UXA had to request their servers be registered. This request was usually performed via an email sent to the IS team requesting the servers be added. After that, however, no interaction with the security team was necessary and security scans could be run and viewed by the UXA at their leisure. COMPL1 (centralized log management), demonstrated the lowest change in behavior between pre- and post-workshop. This metric required sending server log data to the IS team via syslog forwarding. That means that the interaction level, effort required, and data exposure were significantly higher than the other metrics. This level of data sharing may not have been desirable to the UXAs outside of the central IT organization which could account for this metric being the lowest compliance change. Additionally, changes that involved the IS team, may have been limited by the 90-day period of the study. Although quarterly analysis of security metrics was recommended by Jaquith (2007) that time period may not have allowed for the significant number of requests and project load that the IS team experienced after the security workshop. Project delays may have resulted in reduced compliance scores. With additional time, allowing for the project implementation delays of IS team, COMPL1, COMPL2, and COMPL4 implementation may have shown greater

degree of change.

One of the greatest challenges facing this study was the number of participants. UXAs across the institution tend to be very isolated within their own fiefdoms where they maintain complete control. The workshop had 60 individuals that participated but investigation showed that some were not UXAs, and a few were managers and directors that did not administer any servers. This discovery dropped the total participant count to 42 UXAs. While this number still met the levels recommended by Hair et al. (2017) for a PLS-SEM analysis, it may have limited the statistical analyses and generalizability of the results.

It was noted in the data analysis that the four TA-PV questions did not reach significance levels for Cronbach's α , ρ , and AVE. The questions were pulled from work by Hanus and Wu (2016), one question was from the work of Siponen et al. (2014), one question was from the work of Ifinedo (2012), and a final question was developed based on the recommendation of a pilot-tester. While the questions were deemed sufficient by pilot testers, it appears that the four questions did not combine into reliable indicators for the TA-PV construct. The AH survey questions were developed for this study and reviewed by the SME pilot-testers. While VIF and HTMT evaluated all the AH indicators as meeting collinearity constraints, the Cronbach's α was still below the statistical requirement. Last, several participants indicated that there was some confusion regarding the CB question used in the survey. Due to the confusion, the description associated with the question was clarified for the post-workshop survey. At that point, however, the participants had already experienced the question which may have impacted the choices they made.

After the workshop, the ISC was instantiated and made available to participants to allow them to use Metasploit to breach a vulnerable Linux VM. Unfortunately, only 38% of the participants completed the server breaching exercise in the four hours following the workshop. The following week several participants asked for the ISC to be restarted for a few hours, but this only resulted in an additional 4% increase in participation in the Metasploit lab. If the ISC could have remained running 24/7 for the weeks following the workshop, UXA would have had significantly more opportunity to use the Metasploit lab. Unfortunately, due to the cost of running the scenario in AWS, it was not deemed possible to run the lab continuously. Finally, had the workshop been in-person as initially planned it would have been easier to encourage participation in the ISC. Unfortunately, due to COVID-19, the work sites had been closed and remote training was required.

Implications

This study demonstrated the influence of security training and knowledge sharing on the use of cognitive heuristics and biases of a unique group of systems administrators. UXAs have sometimes been generalized by IS teams as cowboys and renegades. In the institution where the study was performed the UXAs are spread out geographically and organizationally. Many participants managed a handful of servers with minimal interaction with the IS team. The security workshop brought together many of these individuals from across the institution to help them become aware of the vulnerabilities facing UNIX servers and the risks associated with not implementing security. Additionally, the workshop introduced participants to the key actions they can implement and the tools they can use to protect their UNIX servers. The post-workshop security updates provided news about newly identified vulnerabilities, recent breaches, and more

guidance on how to implement security tools discussed in the workshop. The goal of the post-workshop security updates was to maintain security awareness and encourage the implementation of security controls. The feedback from participants regarding the content of the workshop and security updates was consistently positive. The interaction of the participants in the new Microsoft Teams channel was also encouraging. Clearly, from an organizational perspective, institutions that have UXAs need to provide security awareness training that is relevant and provides the UXAs the knowledge and tools they need to improve the security of UNIX servers. Additionally, there seems to be a desire for a sense of community even among the distributed UXAs in the organization. The periodic emails asking for other UXAs' advice and the use of the Teams channel demonstrated that shared knowledge helped everyone secure their servers. Last, the IS team needs to try to approach UXAs to help them integrate into the organizations overall IS strategy. At the organization studied, the IS team is largely focused on the threats and vulnerabilities facing Windows servers. This lack of UNIX focus by the IS team leaves some UXAs feeling overlooked and underappreciated and could lead to dangerous levels of non-compliance. The workshop, ISC, and security update emails demonstrated the value for UXAs to connect with the IS team. Additionally, it helped show the importance of embracing IS tools that protect the organization.

Recommendations

Several recommendations can be made to further this line of research. First, increasing the number of participants would increase the statistical relevance of the study and could potentially demonstrate the impact that OB has on actual security compliance behavior. The challenge is that most organizations have a limited number of UXAs so

doing this research across organizations might be necessary. This would, however, introduce the new challenge of gathering the behavioral metrics on servers in different organizations. It is possible that a scoring script could be developed that runs on all the participant's servers and they send the results to the researcher. Second, setting up the ISC on premise would allow it to remain operational for the weeks following the workshop potentially increasing participation. The hope in completing the ISC was to demonstrate to the UXAs how easy it was to breach a vulnerable Linux VM using Metasploit. Unfortunately, the limited availability of the ISC seemed to reduce participation. Third, modifying the TA-PV questions to come from a single, reliable, and validated survey instrument may resolve the Cronbach's α and ρ problems associated with this study's TA-PV indicator questions. Fourth, it might be helpful to do additional testing of the AH questions in an attempt to improve their reliability and validity. Fifth, performing this study as a longitudinal study over a longer period of time may allow for additional implementation of security controls. Finally, performing this study with both Windows administrators and UXAs might afford an opportunity to assess the differences between the two groups in terms of their perceptions of security, vulnerability, severity, and overall security strategy they each employ.

Summary

The implementation of security controls is crucial to the defense of computing systems (Siponen et al., 2014; Tsohou et al., 2015). Organizations are at risk if employees do not follow ISPs and breaches occur (HIPAA Journal, 2020; Ponemon Institute, 2019; Yoo et al., 2018). Many organizations' servers are Windows based, but a significant number of larger, back-end servers are UNIX based to capitalize on increased server

processing power, reliability, security, and clustering technology (Bajgoric, 2006; Beuchelt, 2017a; Hussain et al., 2015). Linux servers represent more than 70% of the web servers used on our planet (W3Techs, 2020). While many vulnerabilities and breaches involve Windows servers and applications, the proliferation of Linux and UNIX servers and their use for back-end databases make them tempting targets for attackers (Newman, 2019; Shrivastava, 2018). Unfortunately, due to the open nature of Linux and UNIX systems, they have a significant number of known vulnerabilities and must be patched and properly secured to mitigate risk (CVE Details, 2020). The problem is that some UXAs fail to completely implement organizational ISP due to the use of cognitive heuristics and biases that lead them to perceive lower threat levels facing Linux and UNIX servers (Siponen et al., 2014; Tsohou et al., 2015). This failure may leave their servers open to systems disruption, loss of proprietary data, cause harm to organizational reputation, and create financial loss due to litigation and fines levied against their organizations (Donaldson et al., 2015; Kraemer & Carayon, 2007). The goal of this research was to empirically assess the effect of a focused SETA workshop, an ISC, and periodic security update emails on UXAs' knowledge sharing, use of cognitive heuristics, biases, threat appraisal, coping appraisal, and ISP compliance behavior.

The following research question guided the investigation: How does a focused SETA workshop, ISC, and regular security updates, designed for UXAs, influence their ISKS, use of cognitive heuristics and biases, and actual ISP compliance behavior? The use of cognitive heuristics and biases can negatively impact threat appraisal and coping appraisals (Kahneman, 2011; Tversky & Kahneman, 1974). Being unaware of the risks facing their servers may result in insufficiently protected UNIX servers due to failure to

comply with ISPs (Albrechtsen & Hovden, 2010; Ki-Aries & Faily, 2017; Renaud, 2012). While generalized SETA programs are useful in organizations for staff-wide training, developing a focused SETA programs and ISC, aimed specifically for the job tasks of UXA, may improve engagement and ISP compliance behavior (Chen et al., 2018; Ki-Aries & Faily, 2017). This research helped to develop an understanding of how a SETA programs, ISC, and periodic security update emails, influenced UXA use of the AH, OB, and CB.

The research took place in several phases. First, the research problem was identified, and a literature review was performed to demonstrate the need and to place this research in the existing body of knowledge. Next, a survey instrument was developed, based largely on prior research, and tested with a pilot group of subject matter experts. After results were returned the survey instrument was modified. The final instrument had 25 questions related to the following constructs: CA-SE, CA-RE, TA-PV, TA-PS, ISKS, OB, AH, and CB. The compliance metrics were also developed during this period. The metrics were based on materials covered during the workshop and reinforced through the security update emails. The five data points evaluated included: the percentage of an administrator's servers sending data to centralized log management system, the percentage of an administrator's servers with centrally recorded Tenable Nessus data, the percentage of an administrator's servers blocking telnet/ftp ports (TCP/UDP 21, 23) and remote services ports (TCP/UDP 512-514), the percentage of an administrator's servers using multi-factor authentication, and the percentage of an administrator's servers that have had recent software updates. These data points were collected through elevated security access to the Tenable Nessus, Splunk, and

organization secure secret databases. Scripts were also used to collect some data points that were unavailable through Tenable.

During this period, the security workshop was developed. The goals of the workshop were to:

- 6) Help maintain cybersecurity awareness by:
 - a. Discussing the scope and impact of data breaches,
 - b. Learning about key websites that provide critical and timely information about software and hardware vulnerabilities,
 - i. Verizon Data Breach Investigations Report (Verizon, 2019),
 - ii. Privacy Rights Clearinghouse (n.d.),
 - iii. U.S. Department of Health and Human Services Office for Civil Rights Breach Portal,
 - iv. National Vulnerability Database.
 - c. Identifying different types of cyber attackers and their motivations,
 - d. Learning about cyber-attacks made against our organization,
 - e. Discussing the cost of a HIPAA breach,
 - f. Discussing our implementation of Defense in Depth
 - i. Firewalls/Intrusion prevention systems (IPS),
 - ii. Security Event/Information Management (SIEM),
 - iii. Identity and rights management,
 - iv. Anti-phishing campaigns,
 - v. Advanced endpoint protection,
 - vi. Threat intelligence,

- vii. Behavioral analytics,
- viii. Penetration testing,
- ix. Cyber forensics.

7) Help participants mitigate security risk for their servers by:

- a. Reviewing the phases of cyber-attacks and threats typically used to exploit servers,
 - i. Reconnaissance,
 - ii. Intrusion,
 - iii. Exploitation,
 - iv. Escalate privilege,
 - v. Lateral movement,
 - vi. Anti-forensics,
 - vii. Denial of service,
 - viii. Data exfiltration.
- b. Discussing the types of cyber attackers
 - i. Cyber criminals – identity theft and financial fraud with goal of monetary gain,
 - ii. Script kiddies – minimal skills, use available exploit kits,
 - iii. Brokers – uncover vulnerabilities in software or systems and sell the information,
 - iv. Insiders – employees, partners, and contractors motivated by perceived wrong,
 - v. Competitors – individuals and organizations seeking to gain

- competitive advantage,
- vi. Cyberterrorists – disable and disrupt network or computing infrastructure,
- vii. Organized crime – highly funded, high-level of skill, seek financial gain,
- viii. Hacktivists – political, social, or principle-based agenda,
- ix. State-sponsored attackers / nation state – highly funded and skilled, intelligence gathering or service disruption, focus is government interests.
- c. Identifying the top threats and risks facing our organization's servers,
 - i. Key threats and vulnerabilities
 1. Compromised credentials and privilege escalation,
 2. Web service exploitation,
 3. Server vulnerabilities that permit remote code execution,
 4. Cryptography weaknesses,
 5. Deserialization,
 6. Scripting,
 7. Malware, fileless malware, and rootkits.
 - ii. Key exploits facing servers
 1. Buffer and stack overflows,
 2. Memory corruption,
 3. Race conditions,
 4. SQL injection.

- d. Identifying 12 activities, settings, and tools participants can use to improve the safety and security of their servers,
 - i. Minimize services / disable unwanted services / limit open ports to reduce vulnerabilities and attack vectors,
 - ii. Remove unnecessary software to reduce the number of vulnerabilities and potential attack vectors,
 - iii. Keep Linux/UNIX kernel and other software as up to date as possible,
 - iv. Ensure strong password policies and account management,
 - v. Kernel hardening to protect against attacks,
 - vi. Configure the server's local firewall,
 - vii. Disk security – file integrity checking, file system encryption,
 - viii. Configure SSH security settings,
 - ix. Implement Security Enhanced Linux,
 - x. Configure centralized log management,
 - xi. Perform monthly vulnerability scans on servers,
 - xii. Run Malware detection software to detect worms, viruses, and rootkits.
 - e. Learning about available enterprise tools and other locally administered tools participants can use for vulnerability analysis and security monitoring.
- 8) See how to perform basic penetration testing and server analysis using common tools by:

- a. Using nmap for enumeration, scanning, and vulnerability analysis on servers,
 - i. Ping scan,
 - ii. Version scan,
 - iii. Vulnerability scan.
- b. Using Wireshark for network traffic analysis for security monitoring and problem resolution,
 - i. Search and filter options,
 - ii. Protocol inspection,
 - iii. Live network traffic capture,
 - iv. Offline network traffic analysis
- c. Using the Metasploit Framework in action and its utility to identify, enumerate, and exploit a server
 - i. Reconnaissance & Scanning/Enumeration,
 - ii. Exploitation demo:
 - 1. VSFTPD,
 - 2. Ssh,
 - 3. Mysql,
 - 4. Samba.

9) Access a cloud-based Cyber lab to:

- d. Get hands-on experience using nmap and the Metasploit Framework (MSF) in a secure, cloud-based virtual environment,
- e. Identify, enumerate, breach, and exploit a Linux VM using MSF tools,

f. Compete to find the most flags on the Linux target machine.

10) Connect with other UNIX administrators to increase knowledge sharing and collaboration:

a. Joining a new Microsoft Team's Team for UXAs in the organization.

Also during this period, the Linux-based Metasploit scenario was designed, created, and tested in the EDURange online AWS environment. Once IRB approval was obtained from both organizations, the IS team provided a comprehensive listing of all UNIX servers in the institution. This data were analyzed to identify UXAs across the institution. All of these UXAs were invited to participate in the workshop and ISC. Forty-two participants met the study's requirements and completed all study protocols. In the next phase, participants completed the Qualtrics survey.

Once all pre-workshop data were collected, the 2.5-hour workshop was scheduled and held via secure Zoom session due to the COVID-19 pandemic. Sixty individuals participated in the workshop but only 42 participants were UXAs and used for this study. Immediately following the workshop the ISC was made available to the participants. Due to the cost of running the multiple scenarios in AWS, access was only provided for the four hours immediately following the workshop. The following week, at the request of several participants, the ISC was restarted for one afternoon. Participation in the ISC was limited to 42%. Over the next 90-days, six security update emails were sent to participants. These emails provided an update regarding recently identified UNIX vulnerabilities, relevant CERT alerts, recent breach announcements, an invitation to join the new Microsoft Teams group set up for UXAs collaboration, as well as guidance on the implementation of the Tripwire and Rootkit Hunter applications. The goals of the security

update emails were to maintain current cybersecurity awareness, increase security knowledge sharing, and reinforce security recommendations made during the workshop. Three months after the workshop, an email was sent to all participants to complete the post-workshop survey. Additionally, the participants' servers were reanalyzed to quantify the changes made by the UXA during the study.

During the analysis phase of the research, the pre-workshop survey results and behavioral data points were analyzed using SmartPLS. PLS-SEM has been used extensively to evaluate complex models in IS (Hanus & Wu, 2016; Ifinedo, 2012; Rhee et al., 2012; Safa & Von Solms, 2016; Safa et al., 2016). Post-workshop survey results and behavioral data were also analyzed in SmartPLS. Finally, a multigroup analysis was done by combining the data from pre-workshop and post-workshop and creating data groups. Each analysis included PLS analysis, reliability and validity tests, bootstrap analysis, and blindfolding analysis. The multigroup analysis also included PLS-MGA analysis. For hypothesis testing of H1-3, the paired t-statistics were used to assess significance. To test hypotheses H4a-H8b the data from the PLS-MGA multigroup bootstrapped path analysis results were used to assess path significance. Hypotheses that were accepted were H1, H3, H5a, H5b, H5c, H5d, H6b, and H7b. H2, H4a, H4b, H6a, H6c, H6d, H7a, H8a, and H8b were rejected. These results indicated that the workshop, ISC, and security update emails did have a significant impact on the use of AH, and CB but not OB.

Additionally, it was noted that all five of the behavioral data points had statistically significant increases in IS compliance behavior. Those data points that could be done solely by the UXA without the participation of the IS team (local firewall implementation, patching, and MFA implementation) showed higher rates of change than

those that required action by the IS team (integration with Tenable Nessus, and Splunk integration).

This study demonstrated the need to consider cognitive biases and heuristics when evaluating the most effect way to improve ISP compliance. It also demonstrated the importance of specialized IS training in the form of a UXA-focused workshop, ISC, and security update emails to increase awareness and improve compliance. The ISKS had a statistically significant impact on all five of the evaluated UXAs compliance behaviors. UXAs use of the AH and CB were influenced by the workshop, ISC, and security update emails. While the influence of the ISKS on OB did not reach an acceptable significance level, the bias did demonstrate significant impact to all four elements of PMT, namely TA-PV, TA-PS, CA-RE, and CA-SE. This research adds to the body of knowledge related to specialized SETA program development, the integration of cognitive biases and heuristics with the PMT framework, and analysis of actual security behavior to assess changes after the ISKS intervention.

Appendix A

Information Security Survey Form

Welcome!

Thank you for agreeing to participate in this UNIX administrator workshop and research project! If you are receiving this survey, it means that you have completed and returned the informed consent form and are ready to participate in this UNIX security workshop and cyber lab.

As a reminder, my name is John McConnell. I am an IT Technical Manager and a doctoral candidate in Information Systems in the College of Computing and Engineering at Nova Southeastern University. My dissertation chair is Martha Snyder, Ph.D., from Nova Southeastern University. My research is a study on UNIX systems administrator perceptions about information security, security training, understanding of security risks and vulnerabilities, organizational support, and policy compliance. The Institutional Review Board approval number for this research project is (JHH Application No.: IRB00240988, NSU Application No.: 2020-60).

Completing this survey is an important part of this research project and we appreciate your help in completing this survey. No identifying information will be included in the research report and your responses will be confidential. It should take no longer than 10 minutes to answer the questions. Several questions have a time limitation on them. For those questions please make your choices as quickly as possible in the time provided.

If you have any questions or concerns, you may contact John McConnell (jmconn3@jhmi.edu or jm3967@mynsu.nova.edu) or 410-935-5657. You may also contact my dissertation chair, Martha Snyder, Ph.D. at smithmt@nova.edu or 954-262-2074.

For each question, please honestly rate your level of agreement from strongly disagree (1) to strongly agree (7).

Please click the link below to begin the online survey.

Q5. I believe I have the expertise to implement preventative measures to stop unauthorized people from getting my organization's confidential information stored on my servers.

Q6. I believe I have the skills to implement preventative measures to stop unauthorized people from damaging my servers.

Q7. I believe I can configure my server to provide good protection from software attacks.

Q8. Enabling security measures on my servers will prevent users from gaining unauthorized access to important personal, financial, or patient information.

Q9. The preventative measures available to me to stop people from gaining access to my organization's servers and data are adequate.

- Q10. Frequently applying security patches on my operating system is an effective way of preventing hacker attacks on my servers.
- Q11. My servers could be at risk of having Malware, virus, or similar infection
- Q12. My organization could be subjected to a serious information security threat.
- Q13. I believe that trying to protect my company's servers and information will mitigate the risk of illegal access to organizational data.
- Q14. I believe that all computer systems are potentially vulnerable to malicious activity and compromise.
- Q15. An information security breach in my organization would be cause serious complications for my organization and me.
- Q16. I believe that having my servers infected with malware, a virus, or similar infection would cause serious complications for my organization and me.
- Q17. An information security breach in my organization would cause serious complications for my organization and me.
- Q18. I frequently share my information security knowledge in my team in order to decrease information security risk.
- Q19. I think information security knowledge sharing with my team helps me to understand the usefulness of information security policies in my organization.
- Q20. I think sharing information security knowledge is a valuable practice in my organization.
- Q21. My organization has the tools in place to mitigate information security threats.
- Q22. My organization executable security practices to mitigate information security threats.
- Q23. The likelihood that my servers will be disrupted due to information security breaches in the next 12 months is low.
- Q24. On the next screen you will be presented with four questions. You will be limited to 30 seconds to select your answers. The choices are the same as the previous responses 1-strongly disagree, 2-disagree, 3-somewhat disagree, 4-neither agree nor disagree, 5-somewhat agree, 6-agree, and 7-strongly agree.
- Q25. <Undisplayed timing>
- Q26. I believe Microsoft Windows servers have more vulnerabilities than Linux/UNIX servers.
- Q27. I believe there are more security vulnerabilities, alerts, and patches related to Microsoft Windows servers than Linux/UNIX servers.
- Q28. I believe a Microsoft Windows server containing Protected Health Information (PHI) is likely to be breached.
- Q29. I believe a Linux/UNIX server containing Protected Health Information (PHI) is likely to be breached.
- Q30. Scenario Question: Your organization plans on implementing a new web server to provide customers' access to HIPAA protected PHI data. In order to provide the highest level of security, would you recommend the web server be implemented on the Microsoft Windows or UNIX/Linux operating system? UNIX/Linux Windows

Q31. On the next screen you will be presented with additional information you can choose to review that you might consider regarding your recommendation. There are 12 data points that are either pro (in favor of) or con (against) each operating system. You must choose at least one item and may choose up to 6 items. You are limited to 20 seconds to make your selection. Once you make your selection, click the arrow to move to the next screen. At that time you will be shown the additional information you requested.

Q32. Please select at least one and no more than six additional pieces of information below.

UNIX/Linux (Pro)	UNIX/Linux (Con)	Windows (Pro)	Windows (Con)
UNIX/Linux (Con)	UNIX/Linux (Pro)	Windows (Con)	Windows (Pro)
UNIX/Linux (Pro)	UNIX/Linux (Con)	Windows (Pro)	Windows (Con)

Q33. <Undisplayed timing>

The following are displayed based on display logic. Only items selected in Q32 are displayed.

Q34. UNIX/LINUX (Pro) - UNIX/Linux servers can be configured with higher amounts of memory and CPUs making them significantly more powerful than Windows servers.

Q35. UNIX/LINUX (Con) - Porting of applications to UNIX/Linux distributions is not the focus of many software companies.

Q36. UNIX/LINUX (Pro) - There are fewer demands on the hardware due to reduced operating systems overhead in UNIX/Linux.

Q37. UNIX/Linux (Con) - Several professional office programs (i.e. Microsoft Windows, Microsoft SharePoint, and Microsoft Visio) do not work with UNIX/Linux.

Q38. UNIX/Linux (Pro) - Remote function access is integrated into the native operating system on UNIX/Linux distributions (shell and terminal).

Q39. UNIX/Linux (Con) - UNIX/Linux can be more difficult to administer due to its command line nature.

Q40. Windows (Pro) - A Windows server is easier for new systems administrators due to the intuitive operations of the graphical user interface.

Q41. Windows (Con) - The licensing costs for Windows can be high and can increase with each user.

Q42. Windows (Pro) - Windows is compatible with popular Microsoft programs like SharePoint, Visio, and Exchange.

Q43. Windows (Con) - Windows servers are very vulnerable to malware.

Q44. Windows (Pro) - There are many skilled individuals that can fill Windows systems administrator positions.

Q45. Windows (Con) - The use of mandatory graphical user interface on Windows servers results in significant resource utilization for basic operating systems function.

Q46. Based on the additional information you received, which operating system would you suggest for this Web server? UNIX/Linux Windows

Q47. What category includes your age?

17-24

25-34

35-44

45-65

66 or over

Q48. Thank you for taking the time to complete this survey! Your responses will help us understand how systems administrator perceive information security, security training, security risks and vulnerabilities, and security policy compliance!

Appendix B

UNIX Administrator Interactive Security Challenge

Course Title: UXA Interactive Security Challenge

Delivery Method: Windows or Linux computer and Internet access

Overarching Goal: The overarching goal of this security challenge is to increase security awareness and ISP policy compliance by developing skills needed to do network and server enumeration to facilitate exploitation of a Linux VM in a segregated, cloud environment.

Background: UXAs have the highest privilege levels and access to the vast amount of confidential PHI and PII stored on their servers (Beuchelt, 2017b; Kraemer & Carayon, 2007). They are responsible for operating system installation, configuration, patching, user management, monitoring, data backup, implementation of security controls, disaster recovery, and testing (Beuchelt, 2017b; Inshanally, 2018; Santara, 2013). SETA programs are a means for organizations to minimize the risk of insider caused security failures (Burns et al., 2015; Ki-Aries & Faily, 2017). Users are the weakest link for information security and SETA programs can help to reduce the potential attack surface of organizations by improving the ability of users to identify and prevent information security breaches (Furnell & Clarke, 2012; Gardner & Thomas, 2014). Developing an understanding of the tools used to perform penetration testing may clarify the importance of securing UNIX servers.

Target Audience: The target audience for this security workshop is organizational UXAs.

Length of Course: 2.5 hours

Challenge Description: The goal of the UXA ISC is to develop hands-on skills in penetration testing using tools learned during the security workshop. Learning and using the tools of a penetration tester will encourage participants to think like the hacker so that they develop a security mindset aware of the threats, risks, and vulnerabilities facing their servers and organization. By learning about the common tools and how easily one can identify and enumerate server vulnerabilities the challenge may encourage the development of an information security culture in the UNIX team. The hands-on workshop will demonstrate the need for constant monitoring of vulnerabilities and ultimately the vital need to secure UNIX servers in the organization to prevent loss. Providing an isolated, remote lab environment is an effective training method for systems administrators (Herold, 2011).

ISC Setup: Two Linux VMs will be instantiated for each participant: a participant VM (meta_nat) and a target server (metasploitable). A private subnet will be created between the two VMs. Also an Internet-accessible public subnet for logging/communicating with EDURange. The metasploitable VM is a metasploitable3 image from Rapid7.

Module Learning Objectives: At the end of this ISC module, the participants will:

- 1) be able to perform network reconnaissance, server enumeration, port and service enumeration using nmap to identify a vulnerable Linux server on an isolated network;
- 2) be able to run the Metasploit framework on a Linux VM;
- 3) be able to identify a relevant exploit to use to gain command line access to a Linux server.

Module Setup: For this module, participants will scan the network segment, identify the vulnerable server (metasploitable), and enumerate potential exploits. Then participants will breach metasploitable using as many exploits they can find. Once participants gain access to the VM they will locate, download, decode, and hash CTF target files. Hash values will be used in the EDURange scenario grading system to assess completion of the module.

Learning Objective 1: Participants will be able to perform network reconnaissance, server enumeration, port and service enumeration using nmap to identify a vulnerable Linux server on an enclosed, cloud environment.

- 1) Participants will use the Linux VM (meta_nat).
- 2) Participants will use nmap scan to identify servers, open ports, services on ports, and OS guesses on servers in the isolated EDURange network segment (metasploitable).
- 3) Participants will identify potential targets (IP, open ports, and open services) in the virtual network.

Learning Objective 2: Participants will learn how to perform a server attack using the Metasploit Framework.

- 1) Participants will locate and start the Metasploit Framework in their VM.
- 2) Participants will identify an exploit in the Metasploit framework they will use on the target Linux VM (metasploitable).
- 3) Using Metasploit the participants will gain login access to the Linux VM.
- 4) Once participants gain access to the VM they will locate, download, decode, and hash CTF target files. Hash values will be used in the EDURange scenario grading system to assess completion of the module.

Appendix C

ISC Instruction Sheet

Metasploitable Exercise Guide

Description

Metasploitable poses the challenge of identifying a vulnerable server, enumerating the services and ports, and using the Metasploit Framework to gain access to the server. Finally, you will locate CTF target cards and provide the hashes of the image files for scoring.

Background

Identifying servers on your network and determining their vulnerabilities is an important skill for penetration testers and system administrators. Using tools, like nmap and the Metasploit Framework, you can learn about the threats to your servers. The nmap tool, or network mapper, is a comprehensive, free, open source network scanning tool. It is used by penetration testers, network administrators, and hackers to examine a server. It can be used on a single host or a network segment/IP range. Nmap manipulates TCP flags to elicit information. By analyzing TCP and UDP probes and comparing them against fingerprints of defined responses nmap can:

- detect/discover live hosts on a network (server/host discovery),
- identify active UDP and TCP ports (port enumeration)
- identify software version information for open ports (service discovery)
- identify operating system information
- detect potential vulnerabilities and security holes.

The Metasploit Framework is a part of Kali Linux or can be installed separately on Windows or Linux/UNIX operating systems. It provides a platform that can be used for penetration testing. Metasploit can help to identify, validate, and exploit known vulnerabilities in operating systems, applications, and hardware. It can also be used to develop new exploits.

Three key components are:

- **Exploits** – the method of exploiting a vulnerability in an asset.
- **Payloads** – the code that can be run on a target that has been compromised.
- **Auxiliary modules** – the programs that can perform fuzzing, scanning, and sniffing.

Learning Objectives

At the end of this scenario, the participants will:

- 1) be able to perform network reconnaissance, server enumeration, port and service enumeration using nmap to identify a vulnerable Linux server on an isolated network
- 2) be able to run the Metasploit framework on a Linux VM
- 3) be able to identify a relevant exploit to use to gain command line access to a Linux server
- 4) locate and hash any of the following cards: 8 of clubs, 3 of hearts, 2 of spades, 10 of spades, king of spades, 10 of clubs, 5 of hearts, 5 of diamonds, 9 of diamonds, 6 of clubs, joker, ace of clubs, 8 of hearts, 7 of diamonds.

Instructions

Connect to the NAT VM in EDURange (AWS) using ssh with the user id and password you were provided. Once you have gained knowledge about your VM, you need to look on the closed network (10.0.*) to find the other VM that is your potential target. Use nmap to scan the network and find the available server. Once you have identified the server you then need to gain additional information about the server including open ports, services running on those ports, versions of software running on those ports. Again, you can use nmap to perform all these actions. Once you have detailed as much information about the target as possible, you can turn to the Metasploit Framework to identify potential exploits and breach the server.

Typical process:

- 1) Gain info about your VM (Linux commands)
- 2) Identify the servers on the network segment (nmap ping scan).
- 3) Identify the open ports and software versions on the target (nmap version scan).
- 4) Search Metasploit for exploits, auxiliary modules, and payloads for the identified services.
- 5) Attempt to gain access to the target server (MSF, Web/SQL Injection)
- 6) Identify other accounts on the system (/etc/passwd, /etc/shadow).
- 7) Find a way to escalate privilege to gain root access.
- 8) Locate/find the CTF target files.
- 9) Perform any work needed on the CTF target files so that you can hash the file (md5sum).

A key feature of MSF is the ability to search. Below are some examples of searches you might perform:

```
msf5> search ftp
```

- returns exploits, auxiliary modules, and payloads

```
msf5> search mysql
```

- returns exploits, auxiliary modules, and payloads

```
msf5> search ssh_login
```

- returns auxiliary modules

Other key MSF commands are:

```
msf5 > use auxiliary/scanner/ftp/ftp_version
```

- If successful, this would set your context to this exploit. You can see that this happened by looking at the new prompt.

```
msf5 auxiliary(scanner/ftp/ftp_version) > show options
```

- Shows you the options that are available for the specific context

```
msf5 auxiliary(scanner/ftp/ftp_version) > back
```

- Change context back one level

```
msf5> set RHOSTS ip-address
```

- Sets the remote host to be the specific ip-address

```
msf5> exploit
```

- Attempts the current exploit.

```
msf5> quit
```

- Exits msfconsole.

You can also run some Linux commands while in the msfconsole including: `pwd`, `ls`, `cat`. This can be helpful if you want to work with user id files or password files.

Also, once you are using an exploit that gains you access to a server, you can try to run OS commands to get additional information.

Hints

Using nmap hints:

- `nmap -sn 10.0.1-50.0-50`
 - performs a ping scan on all IPs in the specified range
 - output indicates all IPs that respond to the ping scan and
 - MAC address.
- `nmap -sV 10.0.0.1`
 - Output includes port, state, service, version for TCP ports, and MAC address.
- `nmap -sT -sV -sC -v -p ports-to-scan --reason --open ip-address`
 - Output includes specific ports, states, services, and versions of software for TCP ports for the specified ip-address.

Gaining access hints:

- FTP is a great avenue for accessing the system and identifying the usernames.
- For FTP try the payload: `cmd/unix/reverse_perl`. Also, to get around a permissions issue on the server, set `SITEPATH /var/www/html/`. Get the user list and move on to the `ssh_login` exploit.
- Using an `ssh_login` scanner is a great way to attempt passwords to gain access.
- Use a SQL injection to attack a website on the target using lynx (a text browser).

Escalation hints:

- Gain access to the server and get a dump of the `/etc/passwd` file to identify users.

- Use the `ssh_login` scanner's different options to attempt different passwords (i.e. blank passwords, `userid=password`, etc.).
- If you get access to the remote system, check to see if you can use `sudo` to switch to root (`sudo -s`).
- Get access to the `/etc/shadow` file to identify password hashes and use John to try and hack passwords.

SQL Injection hints:

- There are typical attacks that can be used to enumerate the users on the system. (And other info if you are diligent!).
- Incorrectly filtered escape characters (see https://en.wikipedia.org/wiki/SQL_injection):

This form of injection occurs when user input is not filtered for escape characters and is then passed into an SQL statement. This results in the potential manipulation of the statements performed on the database by the end-user of the application.

The following line of code illustrates this vulnerability:

```
statement = "SELECT * FROM users WHERE name = " + userName + ";
```

This SQL code is designed to pull up the records of the specified username from its table of users. However, if the "userName" variable is crafted in a specific way by a malicious user, the SQL statement may do more than the code author intended. For example, setting the "userName" variable as: `' OR '1'=1` renders one of the following SQL statements by the parent language:

```
SELECT * FROM users WHERE name = " OR '1'=1';
```

```
SELECT * FROM users WHERE name = " OR '1'='1' -- ';
```

If this code were to be used in an authentication procedure then this example could be used to force the selection of every data field (*) from all users rather than from one specific user name as the coder intended, because the evaluation of '1'='1' is always true.

It is also possible to use the UNION SELECT to pull data from database tables using (for example):

```
' OR 1=1 UNION SELECT null,null,username,password FROM users#
```

File work hints:

- Files may be txt, zip, wav, pcapng. And some may be hidden inside files! Some may be hidden in super-secret directories and not named like a card!
- Some of the files can be hashed as is to get the answer. Some, however, require some work.
- Exfiltrate the files from the target VM to your NAT VM. Then exfiltrated the files to your local computer to view the files (to verify if they are viewable without modification or require modifications).
- Use md5sum to get the hash of the file.
- Tools that might be helpful working on the more difficult files: exiftool, binwalk, fcrackzip, gimp, Wireshark, base64, and mount.

Appendix D

Security Update Emails

May UNIX/Linux Security Update

Good afternoon!

As we close out May I wanted to share some security updates with you!

Common Vulnerabilities Update

We talked about the importance of keeping up awareness about vulnerabilities and how frequently they are identified. To that end, I thought I would share how things have changed since our meeting on 5/19!

Date	New Vulnerabilities	Updated Vulnerabilities
May 19	34	23
May 20	40	32
May 21	62	29
May 22	138	24
May 23	25	43
May 24	2	21
May 25	9	11

Impacted software includes Apache, Docker, json, Python, Fedora, Ubuntu, and many others. This information is available at: https://cve.mitre.org/cve/data_feeds.html

US-CERT-Alert (AA20-133A) Top 10 Routinely Exploited Vulnerabilities

Take a look at this CERT: <https://www.us-cert.gov/ncas/alerts/aa20-133a>.

Interestingly, the most exploited vulnerabilities from 2016-2019 were vulnerabilities that were found in 2012 (1), 2015 (1), 2017 (5), 2018 (2), 2019 (1)! **Constant vigilance & regular patching** are key to cybersecurity!

2020 Verizon Data Breach Investigations Report

The 2020 Verizon Data Breach Investigations Report was just published. The report analyzed 32,002 incidents and 3,950 confirmed data breaches.

Key updates relevant to our organization:

- 58% of breaches featured hacking (stolen credentials, backdoor, exploited vulnerability, brute force, or buffer overflow) – up from 52%
- Misconfiguration rose to almost 40% for top errors allowing a breach
- 819 incidents and 228 breaches impacted educational institutions
- 798 incidents and 512 breaches impacted healthcare organizations
- Servers continue to be the top target for hackers in the educational/healthcare segments
- Top controls suggested for educational/healthcare institutions: implement a security awareness program, boundary defense, data protection, and secure configurations.
 - Implement a Security Awareness and Training Program (CSC 17) - Educate users about malicious attacks and accidental breaches.
 - Boundary Defense (CSC 12) - Not just firewalls, this control includes network **monitoring**, proxies, and **multifactor authentication**.
 - Data Protection (CSC 13) – Limit data leakage by controlling access to sensitive information. Controls in this list include maintaining an inventory of sensitive information, **encrypting sensitive data**, and limiting/controlling access.

- Secure Configuration (CSC 5, CSC 11) - Ensure and verify that systems are configured with only the **services and access needed to achieve their function.**

Case of the month

The importance of disabling services, implementing server-based firewalls, and securing ssh (implementing defense in depth) can be seen in this recent headline from the news: <https://www.cbronline.com/news/aws-servers-hacked-rootkit-in-the-cloud>

Join the Dialog – Collaborate!

Join the **UNIX/Linux Administrators** Microsoft Team to collaborate and share information amongst your peers in the institutions!

Enterprise Monitoring

If you are interested in implementing Tenable, Splunk, Defender ATP, or other enterprise tools send an email to the monitoring team and they will contact you!

Stay safe!

June Security Update

Greetings!

I hope this email finds you safe and secure! This email is a follow up to the Linux/UNIX Security workshop to give you some additional information about what's going on in the world of Cybersecurity and the impact on us as systems administrators/engineers.

InfraGard FBI Session Info

On May 29th I attended an InfraGard FBI Session whose topic was Securing the Health Sector: Threats to Vaccine Researchers and Manufacturers. The FBI cyber division let us know that there has been a significant increase cyber-attacks related to

COVID 19 research. Targets include academic institutions, biological facilities, bioscience industries, medical facilities, university laboratories, scientific collaborations. China is using open source information (i.e. news articles, company announcements, published research, etc.) to identify potential targets for COVID research data. The recommendations made by the FBI in order of priority included:

- 1) Timely patching of all systems for critical vulnerabilities
- 2) Implementing MFA
- 3) Monitor web applications for unusual activity
- 4) Perform a network baseline analysis

If you are interested in being a part of InfraGard go to this website:

<https://www.infragard.org/>

Server Patch Management

“In years past, Linux server patch management was often thought of in terms of “we don’t patch our servers unless there is a reason to upgrade the version for application compatibility.” This philosophy is no longer appropriate today because of the downtime that can result from malicious code targeting known vulnerabilities on unpatched systems and the concerns around governance and regulatory compliance standards such as HIPAA (Health Insurance Portability and Accountability Act) and SOX (Sarbanes-Oxley Act). Patch management has now become an important buzzword in corporate IT organizations and business offices.” From: Taking A Proactive Approach to Linux Server Patch Management, n.d., https://www.suse.com/media/white-paper/suse_linux_patch_management.pdf

Question: Why disable services and add a local firewall?

I was asked this question after our workshop from an experienced systems

administrator. Honestly, I had to think about it and do a little digging. I also asked a few “security experts” their thoughts. No security control will be 100% effective. There is always a chance that some nefarious individual will find a way around a control. Disabling services, like ftp and telnet, is one way to reduce the potential attack surface. Adding a local firewall adds an additional layer of security to the server. To some that seems like overkill, but the truth is our goal as UNIX/Linux systems administrators is to protect our servers and data the best way we can. With local firewalls being so easily configurable why not make that extra effort?

New Linux Vulnerabilities

From 5/26 to 6/14 there were 1053 new vulnerability identified 648 modifications to known vulnerabilities! Vulnerability counts: Linux 5652/137377 (103 new for 2020), RedHat 11362/137377 (81 new for 2020), Ubuntu 7837/137377 (213 new for 2020), and AIX 352/137377 (2 new for 2020). These stats are a clear indication of the necessity to patch regularly!

National Vulnerability Database: <https://nvd.nist.gov/vuln/search>

10 Linux Kernel Vulnerabilities

The article, “**The Top 10 Linux Kernel Vulnerabilities You Should Know**” by G. Avner (2019) provides some great information regarding Linux kernel vulnerabilities. You can check out this article at the following website:

<https://resources.whitesourcesoftware.com/blog-whitesource/top-10-linux-kernel-vulnerabilities>

Join the Dialog – Collaborate!

Join the **UNIX/Linux Administrators** Microsoft Team to collaborate and share information amongst your peers in the institutions!

As always, please email me if you have any questions, comments, suggestions, or concerns related to Linux/UNIX security!

Stay safe!

July Security Update

Good morning!

I wanted to share another update on what is going on with security!

New ransomware that is targeting Windows and Linux systems

The main targets of Tycoon are organizations in the software and education industries. It is unusual because it is written in Java and deployed as a trojanized JRE. Also it is compiled within a Java image file effectively hiding the malicious intention. The article continues by reaffirming the importance of applying security patches as soon as possible as this can help to prevent ransomware attacks where hackers exploit known vulnerabilities. Here is a link to the whole article:

<https://www.zdnet.com/article/this-new-ransomware-is-targeting-windows-and-linux-pcs-with-a-unique-attack/>

Netgear router vulnerability

Do you have a Netgear router at home? If so, you might want to be aware of a new vulnerability! Looks like they are hoping for a patch to be released soon. Here's a link to the whole article: Unpatched vulnerability identified in 79 Netgear router models:

<https://www.zdnet.com/article/unpatched-vulnerability-identified-in-79-netgear-router->

models/

40 Linux Server Hardening Security Tips

This article provides some key things that Linux/UNIX administrators can do to improve security on their servers. Key items (that we also discussed at the security workshop) include:

- 1) Avoid Using FTP, Telnet, And Rlogin / Rsh Services
- 2) Minimize Software to Minimize Vulnerability
- 3) Keep Linux Kernel and Software Up to Date
- 4) User Accounts and Strong Password Policy
- 5) Disable Unwanted Linux Services
- 6) Configure Iptables and TCPWrappers based Firewall
- 7) Linux Kernel /etc/sysctl.conf Hardening

Here's a link to the full article: <https://www.cyberciti.biz/tips/linux-security.html>

Running RedHat/Centos 6 or 7 or Debian 8?

The Mutagen Astronomy vulnerability has been around for a while (> 10 years). It can allow an attacker to gain root access to the target system. Most distributions have issued patches, but it is critical that the patch be installed to mitigate this vulnerability. Delays in implementing patches (i.e. not keeping software up to date) provides a window for malicious attackers to target your servers. Here is a link to the full article:

<https://www.servercentral.com/blog/linux-vulnerabilities-importance-patching/>

UCSF Pays \$1.14M to NetWalker Hackers After Ransomware Attack

After NetWalker ransomware locked down several servers of its School of Medicine, UCSF paid the hackers' ransom demand to decrypt the data and restore function to the

impacted systems. Here is a link to the full article:

<https://healthitsecurity.com/news/ucsf-pays-1.14m-to-netwalker-hackers-after-ransomware-attack>

National Vulnerabilities Database Dashboard

Just a quick reminder about the NVD dashboard as a great place to learn about new vulnerabilities. Here is a link to the website: <https://nvd.nist.gov/general/nvd-dashboard>

Since the workshop on 5/19 the following new vulnerabilities were announced: RedHat: 37, Ubuntu: 38, AIX: 2, Gentoo: 58, Apache: 18, MySQL: 7, and Cisco: 119. Again, emphasizes the need for regular patching and updates!

SANS Webcast on Securing Containers

If you join the SANS organization, they regularly have free security related webinars.

One that I saw that I wanted to pass on was on securing containers.

<https://www.sans.org/webcasts/containers-vulnerability-management-time-step-things-up-115850>

F5 Vulnerability CVSS 10

A vulnerability that allows for remote code execution was discovered in F5 BIG-IP devices. It is unusual for a vulnerability to get a CVSS score of 10 so I thought I would share it with you. Below is a link to the full story:

<https://www.zdnet.com/google-amp/article/f5-patches-vulnerability-that-received-a-cvss-10-severity-score/>

Metasploit Lab Opportunity

If you are interested in getting access to the online lab that lets you try and break into a Linux server using nmap and Metasploit let me know! If a few are interested I could fire

up the lab again for you and leave it up for a week!

Be safe!

August Security Update

Good morning!

Below is your August security update!

Garmin hit by ransomware

On July 23rd, Garmin was hit by a huge ransomware event that resulted in customers losing use of their personal devices as well as aviation navigation devices systems going offline. Here is a link to one article: <https://www.zdnet.com/article/garmin-services-and-production-go-down-after-ransomware-attack/>

InfraGard

On June 21st I participated in a webinar presented by the New York InfraGard team regarding cyber threats in the time of COVID. They discussed several recent breaches that included passive surveillance followed by sniper strikes—focused on Citrix Netscalers and Cisco routers. They emphasized the importance of business continuity planning in recovering from breaches and ransomware. Additionally, they said that off-site, off-line backups have helped several organizations that had their on-line backups encrypted by the ransomware too!

InfraGard is a non-profit program by the FBI in partnership with private industry. They periodically have web sessions, talks, and conferences that are a great opportunity to meet folks and learn about what threats are out there. Attached are a couple of information FAQs and brochures on the organization.

National Cyber League

The NCL has Cyber Games several times a year. It is a great opportunity to think like a hacker and learn to use some great tools and applications. The sections included in the NCL include cryptography, enumeration and exploitation, log analysis, network traffic analysis, open source intelligence, password cracking, scanning, web application exploitation, and wireless access exploitation. Prior to the actual game event participants are given access to the “gym” to learn about the different areas and what tools might be useful answer each question. I have done it several times and always enjoy the challenge. You can also get an official Score Card that can give you a picture of your increased knowledge each game. Here’s a link to their website: <https://nationalcyberleague.org/>

Centralized Log Management

During the workshop we talked about the importance of centralized log management in analyzing logs if you manage multiple servers. For the enterprise we use Splunk. There are, however, several tools that you can use to create your own log management environment for the servers you manage. The article below is a good introduction to Elk Logstash should you want to create your own:

<https://www.howtoforge.com/tutorial/how-to-setup-elk-logstash-as-centralized-log-management-server/>

Number of Patient Records

According to U.S. Department of Health and Human Services Office for Civil Rights Breach Portal the number of patient records that have been lost/stolen since January 1, 2020 is a staggering 6,620,720 records! Almost 250 organizations were impacted by the breaches.

Stolen Logins

Business Insider reported that hackers are selling more than 15 billion stolen login credentials on the dark web. Stolen credentials can sell for anywhere from \$1 to \$140,000 depending on the type of account. They continued by recommending that organizations and individuals use password manager applications, **enable two-factor authentication**, and **regularly change passwords** to reduce the risk of stolen credential attacks. The link to the full article is below:

<https://www.businessinsider.com/hackers-circulating-15-billion-stolen-logins-on-the-dark-web-2020-7>

Sharpen your skills

Did you know that there are multiple Linux OS courses, as well as other Linux Security, Kali Linux, and Ethical Hacking classes available to employees through LinkedIn Learning and MyLearning? I am currently taking a great class for the CompTIA Linux+ exam. It is important to keep your skills up to date as technologies change! Below are security recommendations from the Linux+ exam course (hopefully a few sound familiar!):

Manage Installed and Running Services

- Uninstall any software that is not necessary
- Disable any running services that are not necessary
- Be diligent on OS security updates
- Disable insecure services such as FTP, Telnet, and Finger
- Always run a firewall
- Use TCP Wrappers for services that provide that support

- Use PAM for granular network access
- Change default service ports
- Restrict remote logins to trusted hosts
- Use VPN connections

RedHat/CentOS BootHole Vulnerability Patch

You may want to hold off on RedHat and CentOS patching related to the BootHole vulnerability. Apparently RedHat and CentOS systems are not booting after application of the BootHole patches. The patches were for GRUB and the kernel. The article below provides information on how to downgrade the affected packages.

<https://arstechnica.com/gadgets/2020/07/red-hat-and-centos-systems-arent-booting-due-to-boothole-patches/>

Join the Dialog – Collaborate!

Join the **UNIX/Linux Administrators** Microsoft Team to collaborate and share information amongst your peers in the institutions! We have almost 40 administrators that have joined the team!

Study Finalization

In a few weeks you will be receiving a link to complete the final study survey associated with this research project. It is very similar to what you did in April/May.

Thanks and be safe!

Appendix E

Permissions for Use of Survey Questions

Approval was requested from the researchers that he developed questions that were modified and used in the present research. The articles referenced and the author's email responses from the authors are shown below.

Siponen, M., Mahmood, M. A., & Pahlila, S. (2014). Employees' adherence to informaton security policy: An exploratory field study. *Information & Management*, 51(2), 217-224.

Mahmood, M. Adam <mmahmood@utep.edu>
Sat 11/9/2019 1:18 PM

John,

You have my permission to use the items you mentioned in your email for your dissertation.

Dr. Adam Mahmood

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security*, 31(1), 83-95.

Ifinedo, P. (2014). Information systems security policy compliance: An empirical study of the effects of socialization, influence, and cognition. *Information & Management*, 51(1), 69-79.

Princely Ifinedo <pifinedo@gmail.com>
Sat 11/9/2019 1:27 PM

Dear John P McConnell,

You're granted permission to items from my 2 papers for your work.

Thank you.

Dr. Ifinedo

Hanus, B., & Wu, Y. (2016). Impact of users' security awareness on desktop security behavior: A protection motivation theory perspective. *Information Systems Management*, 33(1), 2-16.

Bartlomiej Hanus <bartlomiejh@gmail.com>
Sat 11/9/2019 2:02 PM

John,

No problem, you are welcome to use the aforementioned items in your study. I hope they will be helpful to you. Please let me know if you have any further questions.

Thanks,
Bart

Safa, N. S., & Von Solms, R. (2016). An information security knowledge sharing model in organizations. *Computers in Human Behavior*, 57(C), 442-451.

Safa, N. S., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model in organizations. *Computers & Security*, 56, 70-82.

Steven Furnell <S.Furnell@plymouth.ac.uk>
Sat 11/9/2019 1:13 PM

Hi John

I'll leave Nader to give the main authorisation on this, as he was the key author here. However, I do not anticipate a problem.

Please give my regards to Yair.

Best regards

Steve

nader sohrabi safa <sohrabisafa@yahoo.com>
Sat 11/9/2019 9:11 PM

Dear John

you can use the questions from our two models that we published before with citation in your work.

Best Regards
Dr Nader Sohrabi Safa
School of Computing, Electronics and Mathematics

Coventry University, UK

Siponen, M., Mahmood, M. A., & Pahlila, S. (2014). Employees' adherence to information security policy: An exploratory field study. *Information & Management*, 51(2), 217-224.

Siponen, Mikko <mikko.t.siponen@jyu.fi>
Mon 11/11/2019 2:48 AM

Hi John,

It seems to me self-evident that one can use published instrument even without asking a permission from the original authors (assuming that one include a proper citation). For example, if I wrote paper, and I have 200 references, it seems odd to ask everyone can I cite them...

So, I have no problem if you cite (or use) the measures (a normal citation practice assumed).

I hope this helps and good luck with your work.

— Mikko

Mikko Siponen
Ph.D., D.Soc.Sc.
Vice Dean for Research
Professor of Information Systems
University of Jyväskylä
Tel. +358 505588128

Rhee, H., Ryu, Y. U., & Kim, C. (2012). Unrealistic optimism on information security management. *Computers & Security*, 31(2), 221-232.

Young Ryu <ryoung@utdallas.edu>
Fri 11/15/2019 12:45 PM

Dear John,

You have my permission to use the questionnaire.

Young Ryu

Cheongtag Kim <ctkim@snu.ac.kr>
Sun 11/10/2019 6:27 PM

Hello Mr. John McConnell,

Thank you for your interest in our work. In fact, I don't think you need permission to use items published in the academic journal. Anyway, I DO give my permission to use items in Rhee, Ryu, and Kim (2012).

Cheongtag

Appendix F

Information Security Survey – Pilot Form

From Qualtrics:

Dear Reviewer,

Thank you for taking the time to pilot test this survey of UNIX Administrator Cognitive Heuristics and Biases. The goal of this instrument is to better understand how perceived vulnerability, perceived severity, self-efficacy, response efficacy, information security knowledge sharing, confirmation bias, optimistic bias, and the availability heuristic influence UNIX administrator's ISP compliance behavior. Your feedback will help ensure the survey instructions and questions are clear and complete. Please set aside at least 30 minutes to complete your review.

First, review the research summary provided below. Then proceed to review the survey instructions and questions. This survey is divided into nine sections. You will be presented the questions as the participant would see them and then you are asked to review the questions in each section and provide your feedback. You do not have to make selections for the participant questions.

Again, thank you for your time and participation in this important research effort.

Should you have any question, feel free to e-mail me.

Thank you!

John McConnell at jm3967@mynsu.nova.edu

Participants Welcome:

Welcome!

My name is John McConnell. I am a doctoral candidate in Information Systems in the College of Computing and Engineering at Nova Southeastern University. I am also an IT Technical Manager at Johns Hopkins. My dissertation chair is Martha Snyder, Ph.D., from Nova Southeastern University. My research is a study on systems administrator perceptions about information security, security training, understanding of security risks and vulnerabilities, organizational support, and policy compliance. The Institutional Review Board approval number for this research project is (TBD).

You are receiving this survey because you have been identified as a systems administrator working with enterprise class servers in your institution. A systems administrator is an IT specialist that is responsible for operating system installation, configuration, patching, user management, monitoring, data backup, implementation of security controls, disaster recovery, and testing.

The goal is to understand how security training that is tailored toward your day-to-day work helps you effectively secure your servers.

We appreciate your help in completing this survey. Completing it implies your informed consent to participating in this research study. No identifying information will be included in the research report and your responses will be confidential. It should take no longer than 10 to 15 minutes to answer the questions. Several questions have a time limitation on them. For those questions please make your choices as quickly as possible in the time provided.

If you have any questions or concerns, you may contact John McConnell (jmconn3@jhmi.edu or jm3967@mynsu.nova.edu) or 410-935-5657. You may also contact my dissertation chair, Martha Snyder, Ph.D. at smithmt@nova.edu (954)262-2074.

For each question, please honestly rate your level of agreement from strongly disagree (1) to strongly agree (7).

Expert Info - What feedback do you have regarding the participant's welcome?

Expert Information: Section A - Self-Efficacy

Self-efficacy is the belief that one is capable of the adaptation necessary to mitigate the negative event (Rogers & Prentice-Dunn, 1997).

Q2. I believe I have the expertise to implement preventative measures to stop unauthorized people from getting my organization's confidential information stored on my servers.

Keep Adjust Remove

Q3. I believe I have the skills to implement preventative measures to stop unauthorized people from damaging my servers.

Keep Adjust Remove

Q4. I believe I can configure my server to provide good protection from software attacks.

Keep Adjust Remove

Design flow logic – If reviewer selects “2” or “3”: You selected "2. Adjust" and/or "3. Remove" to at least one of the items above. Please provide your recommended adjustments (or "N/A" if none)

Please provide additional questions that you see fit to be included for 'Self-Efficacy' beyond those listed above (or "N/A" if none)

Participant's questions:

Q5. Enabling security measures on my servers will prevent users from gaining unauthorized access to important personal, financial, or patient information.

Q6. The preventative measures available to me to stop people from gaining access to my organization's servers and data are adequate.

Q7. Frequently applying security patches on my operating system is an effective way of preventing hacker attacks on my servers.

Expert Information: Section B - Response-Efficacy

Response efficacy is an evaluation of the effectiveness of the proposed behavior to reduce the probability of the negative event (Rogers & Prentice-Dunn, 1997).

Q8. Enabling security measures on my servers will prevent users from gaining unauthorized access to important personal, financial, or patient information.

Keep Adjust Remove

Q9. The preventative measures available to me to stop people from gaining access to my organization's servers and data are adequate.

Keep Adjust Remove

Q10. Frequently applying security patches on my operating system is an effective way of preventing hacker attacks on my servers.

Keep Adjust Remove

Design flow logic – If reviewer selects “2” or “3”: You selected "2. Adjust" and/or "3. Remove" to at least one of the items above. Please provide your recommended adjustments (or "N/A" if none)

Please provide additional questions that you see fit to be included for ‘Response-Efficacy’ beyond those listed above (or "N/A" if none)

Participant’s questions:

Q11. My servers are at risk of having Malware, virus, or similar infection

Q12. My organization could be subjected to a serious information security threat.

Q13. I believe that trying to protect my company's servers and information will mitigate the risk of illegal access to organizational data.

Q14. I believe that all computer systems are potentially vulnerable to malicious activity and compromise.

Expert Information: Section C - Perceived Vulnerability

Perceived vulnerability is an assessment of probability a negative event will occur if no changes are made to the individual’s behavior (Rogers & Prentice-Dunn, 1997).

Q11. My servers are at risk of having Malware, virus, or similar infection

Keep Adjust Remove

Q12. My organization could be subjected to a serious information security threat.

Keep Adjust Remove

Q13. I believe that trying to protect my company's servers and information will mitigate the risk of illegal access to organizational data.

Keep Adjust Remove

Q14. I believe that all computer systems are potentially vulnerable to malicious activity and compromise.

Keep Adjust Remove

Design flow logic – If reviewer selects “2” or “3”: You selected "2. Adjust" and/or "3. Remove" to at least one of the items above. Please provide your recommended adjustments (or "N/A" if none)

Please provide additional questions that you see fit to be included for ‘Perceived Vulnerability’ beyond those listed above (or "N/A" if none)

Participant’s questions:

- Q15. An information security breach in my organization would be cause serious complications for my organization and me.
- Q16. I believe that having my servers infected with malware, a virus, or similar infection would cause serious complications for my organization and me.
- Q17. An information security breach in my organization would cause serious complications for my organization and me.

Expert Information: Section D - Perceived Severity

Perceived severity is an evaluation of the potential physical, psychological, social, or economic harm an individual expects may occur (Rogers & Prentice-Dunn, 1997).

Q15. An information security breach in my organization would be cause serious complications for my organization and me.

Keep Adjust Remove

Q16. I believe that having my servers infected with malware, a virus, or similar infection would cause serious complications for my organization and me.

Keep Adjust Remove

Q17. An information security breach in my organization would cause serious complications for my organization and me.

Keep Adjust Remove

Design flow logic – If reviewer selects “2” or “3”: You selected "2. Adjust" and/or "3. Remove" to at least one of the items above. Please provide your recommended adjustments (or "N/A" if none)

Please provide additional questions that you see fit to be included for ‘Perceived Severity’ beyond those listed above (or "N/A" if none)

Participant’s questions:

- Q18. I frequently share my information security knowledge in my team in order to decrease information security risk.
- Q19. I think information security knowledge sharing with my team helps me to understand the usefulness of information security policies in my organization.
- Q20. I think sharing information security knowledge is a valuable practice in my organization.

Expert Information: Section E - Information Security Knowledge Sharing

Information security knowledge sharing can help to foster sharing of ideas, experiences, tools, and processes to improve security and protect an organization's information systems assets (Flores, Antonsen, & Ekstedt, 2014).

Q18. I frequently share my information security knowledge in my team in order to decrease information security risk.

Keep Adjust Remove

Q19. I think information security knowledge sharing with my team helps me to understand the usefulness of information security policies in my organization.

Keep Adjust Remove

Q20. I think sharing information security knowledge is a valuable practice in my organization.

Keep Adjust Remove

Design flow logic – If reviewer selects “2” or “3”: You selected "2. Adjust" and/or "3. Remove" to at least one of the items above. Please provide your recommended adjustments (or "N/A" if none)

Please provide additional questions that you see fit to be included for ' Information Security Knowledge Sharing' beyond those listed above (or "N/A" if none)

Participant's questions:

Q21. My organization has the tools in place to mitigate information security threats.

Q22. My organization executable security practices to mitigate information security threats.

Q23. The likelihood that my servers will be disrupted due to information security breaches in the next 12 months is low.

Expert Information: Section F - Optimistic Bias

Optimistic bias leads one to assess situations in self-serving ways (Rhee et al., 2012). Optimistic bias is a protective measure to protect the self, and reduce both anxiety and stress (Rhee et al., 2012).

Q21. My organization has the tools in place to mitigate information security threats.

Keep Adjust Remove

Q22. My organization executable security practices to mitigate information security threats.

Keep Adjust Remove

Q23. The likelihood that my servers will be disrupted due to information security breaches in the next 12 months is low.

Keep Adjust Remove

Design flow logic – If reviewer selects “2” or “3”: You selected "2. Adjust" and/or "3. Remove" to at least one of the items above. Please provide your recommended adjustments (or "N/A" if none)

Please provide additional questions that you see fit to be included for 'Optimistic Bias' beyond those listed above (or "N/A" if none)

Participant's questions:

Q24. On the next screen you will be presented with four questions. You will be limited to 30 seconds to select your answers. The choices are the same as the previous responses 1-strongly disagree, 2-disagree, 3-somewhat disagree, 4-neither agree nor disagree, 5-somewhat agree, 6-agree, and 7-strongly agree.

Q25. <Undisplayed timing>

Q26. I believe Microsoft servers have more vulnerabilities than Linux/UNIX servers.

Q27. I believe there are more security vulnerabilities, alerts, and patches related to Windows servers than Linux/UNIX servers.

Q28. I believe a Windows server containing protected health information (PHI) is likely to be breached.

Q29. I believe a Linux/UNIX server containing protected health information (PHI) is likely to be breached.

Expert Information: Section G - Availability Heuristic

To judge the frequency or probability of an event an individual may assess the availability of associations related to the event (Tversky & Kahneman, 1974). Rather than taking the time to consider an actual probability it is easier to estimate a probability based on the ease that one recalls occurrences of a similar event, termed the availability heuristic (Kahneman, 2011; Kliger & Kudryavtsev, 2010; Tversky & Kahneman, 1974).

I believe Microsoft servers have more vulnerabilities than Linux/UNIX servers.

Keep Adjust Remove

I believe there are more security vulnerabilities, alerts, and patches related to Windows servers than Linux/UNIX servers.

Keep Adjust Remove

I believe a Windows server containing protected health information (PHI) is likely to be breached.

Keep Adjust Remove

I believe a Linux/UNIX server containing protected health information (PHI) is likely to be breached.

Keep Adjust Remove

Design flow logic – If reviewer selects “2” or “3”: You selected "2. Adjust" and/or "3. Remove" to at least one of the items above. Please provide your recommended adjustments (or "N/A" if none)

Please provide additional questions that you see fit to be included for 'Trust' beyond those listed above (or "N/A" if none)

Expert information: Section H - Confirmation Bias:

Confirmatory bias will be tested using a fictional scenario, similar to the technique of Fischer et al., 2011. Fischer et al. (2011) presented a scenario, asked participants to make an initial decision, then provided six confirming and six disconfirming bits of additional information they can choose to review, and then asked to choose again. The level of confirmation bias will be determined by subtracting the number of disconfirming from the confirming choices selected (Fischer et al., 2011).

Participant's questions:

Q30. Scenario Question: Your organization plans on implementing a new web server to provide customers' access to HIPAA protected PHI data. In order to provide the highest level of security, would you recommend the web server be implemented on the Windows or UNIX/Linux operating system?

UNIX/Linux

Windows

Q31. On the next screen you will be presented with additional information you can choose to review that you might consider regarding your recommendation. There are 12 data points that are either pro (in favor of) or con (against) each operating system. You must choose at least one item and may choose up to 6 items. You are limited to 20 seconds to make your selection. Once you make your selection, click the arrow to move to the next screen. At that time you will be shown the additional information you requested.

Q32. Please select at least one and no more than six additional pieces of information below.

UNIX/Linux (Pro)	UNIX/Linux (Con)	Windows (Pro)	Windows (Con)
UNIX/Linux (Con)	UNIX/Linux (Pro)	Windows (Con)	Windows (Pro)
UNIX/Linux (Pro)	UNIX/Linux (Con)	Windows (Pro)	Windows (Con)

Q33. <Undisplayed timing>

The following are displayed based on display logic. Only items selected in Q32 are displayed.

Q34. UNIX/LINUX (Pro) - UNIX/Linux servers can be configured with higher amounts of memory and CPUs making them significantly more powerful than Windows servers.

Q35. UNIX/LINUX (Con) - Porting of applications to UNIX/Linux distributions is not the focus of many software companies.

Q36. UNIX/LINUX (Pro) - There are fewer demands on the hardware due to reduced operating systems overhead in UNIX/Linux.

Q37. UNIX/Linux (Con) - Several professional office programs (i.e. Microsoft Windows, Microsoft SharePoint, and Microsoft Visio) do not work with UNIX/Linux.

Q38. UNIX/Linux (Pro) - Remote function access is integrated into the native operating system on UNIX/Linux distributions (shell and terminal).

Q39. UNIX/Linux (Con) - UNIX/Linux can be more difficult to administer due to its command line nature.

Q40. Windows (Pro) - A Windows server is easier for new systems administrators due to the intuitive operations of the graphical user interface.

Q41. Windows (Con) - The licensing costs for Windows can be high and can increase with each user.

Q42. Windows (Pro) - Windows is compatible with popular Microsoft programs like SharePoint, Visio, and Exchange.

Q43. Windows (Con) - Windows servers are very vulnerable to malware.

Q44. Windows (Pro) - There are many skilled individuals that can fill Windows systems administrator positions.

Q45. Windows (Con) - The use of mandatory graphical user interface on Windows servers results in significant resource utilization for basic operating systems function.

Q46. Based on the additional information you received, which operating system would you suggest for this Web server?

UNIX/Linux

Windows

Expert Information: Section I - Confirmation Bias

Confirmation bias can significantly influence decision making (Kahneman, 2011). With confirmation bias, one gives greater validity to information that supports rather than contradicts one's beliefs (Sternberg, 2004).

What feedback do you have related to the confirmation bias scenario and question?

Participant's questions:

Q47. What category includes your age?

- ☐ 17-24
- ☐ 25-34
- ☐ 35-44
- ☐ 45-65
- ☐ 66 or over

Thank you for taking the time to complete this survey! Your responses will help us understand how systems administrator perceive information security, security training, security risks and vulnerabilities, organizational trust, and security policy compliance!

Expert information:

Do you have any additional feedback for this survey?

Thank you again for taking the time to provide your expert opinion on this survey

instrument! Your input is very helpful to this research project and we sincerely

appreciate it!

Appendix G

IRB Approvals



**Office of Human Subjects Research
Institutional Review Boards**

1620 McElderry Street, Reed Hall, Suite B-130
Baltimore, Maryland 21205-1911
410-955-3008
410-955-4367 Fax
e-mail: jhmeirb@jhmi.edu

Date: March 2, 2020

APPLICATION APPROVAL

Review Type:	Expedited
Principal Investigator:	John McConnell
Number:	IRB00240988
Title:	UNIX Administrator Information Security Policy Compliance: The Influence of a Focused SETA Workshop and Interactive Security Challenges on Heuristics and Biases
Committee Chair:	Susan Bassett
IRB Committee:	IRB-X

Date of Approval: March 2, 2020

Date of Expiration: March 1, 2023

The JHM IRB approved the above-referenced Application.

To keep the JHM IRB application current we are assigning an Expiration Date as noted above. Prior to the expiration date, you will receive an email notification indicating that some action is required. If the Board has determined that a Continuing Review or Progress Report is required, you will need to submit Continuing Review or Progress Report prior to the expiration date. If the Board has determined that No Progress Report is required, you may run the administrative extend approval function.

IRB review included the following:

The Board determined that there is no requirement for continuing review or progress report for this application.

This project has been assigned a 3-year expiration date. You will receive an email notification prior to the expiration date, allowing you to extend this project by completing an 'Extend Approval' activity.

Research on individual or group characteristics or behavior (including, but not limited to, research on perception, cognition, motivation, identity, language, communication, cultural beliefs or practices, and social behavior) or research employing survey, interview, oral history, focus group, program evaluation, human factors evaluation, or quality assurance methodologies.

Changes in Research: All proposed changes to the research must be submitted using a Change in Research application. The changes must be approved by the JHM IRB prior to implementation, with the following exception: changes made to eliminate apparent immediate hazards to participants may be made immediately, and promptly reported to the JHM IRB.

Unanticipated Problems: All unanticipated problems must be submitted using a Protocol Event Report.

If this research has a commercial sponsor, the research may not start until the sponsor and JHU have signed a contract.

Study documents:

Written Consent:

Only consent forms with a valid approval stamp may be presented to participants. All

consent forms signed by subjects enrolled in the study should be retained on file. The Office of Human Subjects Research conducts periodic compliance monitoring of protocol records, and consent documentation is part of such monitoring.

McConnell_IRB00240988_CF_022420_JHMIRB final.docx

Recruitment Materials:

Recruitment email

Additional Supplemental Study Documents:

NSU IRB Approval Letter

Survey

Risk Tier worksheet

Authorization to be PI from department

Institutional Okay to do Study

Protocol:

IT Workshop Learning Objectives

JHM-IRB eForm

Security Challenge Lab

Johns Hopkins Study Team Members: None

The Johns Hopkins Institutions operate under multiple Federal-Wide Assurances: The Johns Hopkins University School of Medicine - FWA00005752, Johns Hopkins Health System and Johns Hopkins Hospital - FWA00006087

Nova Southeastern University IRB Approval

MEMORANDUM

To: **John McConnell**

From: **Ling Wang, Ph.D.,
Center Representative, Institutional Review Board**

Date: **February 10, 2020**

Re: **IRB #: 2020-60; Title, “UNIX Administrator Information Security Policy Compliance: The Influence of a Focused SETA Workshop and Interactive Security Challenges on Heuristics and Biases”**

I have reviewed the above-referenced research protocol at the center level. Based on the information provided, I have determined that this study is exempt from further IRB review under **45 CFR 46.101(b) (Exempt 2: Interviews, surveys, focus groups, observations of public behavior, and other similar methodologies)**. You may proceed with your study as described to the IRB. As principal investigator, you must adhere to the following requirements:

- 1) **CONSENT:** If recruitment procedures include consent forms, they must be obtained in such a manner that they are clearly understood by the subjects and the process affords subjects the opportunity to ask questions, obtain detailed answers from those directly involved in the research, and have sufficient time to consider their participation after they have been provided this information. The subjects must be given a copy of the signed consent document, and a copy must be placed in a secure file separate from de-identified participant information. Record of informed consent must be retained for a minimum of three years from the conclusion of the study.
- 2) **ADVERSE EVENTS/UNANTICIPATED PROBLEMS:** The principal investigator is required to notify the IRB chair and me (954-262-5369 and Ling Wang, Ph.D., respectively) of any adverse reactions or unanticipated events that may develop as a result of this study. Reactions or events may include, but are not limited to, injury, depression as a result of participation in the study, life-threatening situation, death, or loss of confidentiality/anonymity of subject. Approval may be withdrawn if the problem is serious.
- 3) **AMENDMENTS:** Any changes in the study (e.g., procedures, number or types of subjects, consent forms, investigators, etc.) must be approved by the IRB prior to implementation. Please be advised that changes in a study may require further review depending on the nature of the change. Please contact me with any questions regarding amendments or changes to your study.

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

Cc: Marti Snyder, Ph.D.
Ling Wang, Ph.D.

Appendix H

Invitation to Participate

Hello!

I am reaching out to invite you to participate in a new UNIX/Linux security workshop that is focused on securing servers in the Hopkins enterprise. You were identified as a participant because you are a server administrator for Linux or UNIX servers in the configuration management database (CMDB). My name is John McConnell and I work in IT@JH. I am also a doctoral researcher in information security at NSU.

The goal of the workshop is to provide you with information, resources, tools, and practical, hands-on experience to penetration test your own servers and increase security. We will discuss the scope and impact of data breaches, cyber attackers and their motivations, the top threats facing our servers, vulnerability management, penetration testing, and discuss recommendations to help you mitigate risk. Many of the recommendations introduced during the workshop are from the draft Linux/UNIX security standard that is currently being reviewed by the ICSC. Finally, you will also be given the opportunity to perform a penetration test/capture-the-flag challenge on a cloud-based Linux server using the tools we will cover in the workshop.

You are probably aware of some of the tools and resources we will discuss but my hope is that you will walk away from the workshop with some new knowledge and new tools that will help you increase both your cyber awareness and your ability to respond effectively to mitigate security vulnerabilities.

This workshop is also part of my dissertation (Hopkins IRB: IRB00240988, NSU IRB: 2020-60) on UNIX/Linux systems administrator perceptions about information security, security training, understanding of security risks and vulnerabilities, and organizational support.

As this is part of an official study, along with the workshop, there are a few administrative items that need to be completed. Your participation includes completion of an informed consent form, completion of a short pre-workshop survey, participation in the workshop, and an opportunity to exploit a cloud-based Linux server using the Metasploit framework. Finally, you will receive an email to complete a short post-workshop online survey.

As the principal investigator, I will be facilitating the workshop. Darren Lacey, our Chief Information Security Office will also be participating.

Your participation is voluntary, and your participation decision will not affect your employment, education, or training at Johns Hopkins.

The workshop will be held via a secure Zoom meeting Tuesday, May 19th from 9-11 AM. The CTF challenge lab environment will be online from 11-1 PM for those that want to try their hand at penetration testing a Linux server using Metasploit.

I hope you find this workshop to be both informative and fun. It will also introduce you, virtually, to the other UNIX/Linux administrators in the organization. Finally, I plan to create a new Microsoft Teams team called “Hopkins UNIX/Linux Administrators” that you can join for future collaboration.

If you want to participate in this free learning opportunity, please simply reply to this email and I will reserve a space for you!

I hope you will join me to learn something new and to share your experience with other UNIX/Linux administrators!

If you have any questions, please email me.

Appendix I

Combined Inform Consent Form

RESEARCH PARTICIPANT INFORMED CONSENT AND PRIVACY

AUTHORIZATION FORM

Protocol Title: UNIX/Linux Administrator Information Security: The Influence of a Focused SETA Workshop and Interactive Security Challenge

JHH Application No.: IRB00240988

NSU Application No.: 2020-60

Principal Investigator: John McConnell, jmcconn3@jhmi.edu, 667-208-6303.

NSU Faculty Advisor/Dissertation Chair: Marti Snyder, Ph. D

NSU Co-Investigator(s): Yair Levy, Ph. D, Ling Wang, Ph. D.

You are being asked to join a research study. Participation in this study is voluntary. Even if you decide to join now, you can change your mind later.

1. Research Summary:

The information in this section is intended to be an introduction to the study only. Complete details of the study are listed in the sections below. If you are considering participation in the study, the entire document should be discussed with you before you make your final decision.

This research is a study on UNIX/Linux systems administrator perceptions about information security, security training, understanding of security risks and vulnerabilities, and organizational support. The goal is to understand how security training that is tailored toward your day-to-day work helps you improves the security of your servers.

2. Why is this research being done?

This research is being done to assess the effectiveness of a specialized security education training and awareness workshop and hands-on labs on your ability to protect and secure your UNIX/Linux servers. It will also assess how the workshop influences your perception of information security and organizational support.

Who can join this study?

UNIX/Linux systems administrators working with Linux and UNIX servers at Johns Hopkins may participate. A systems administrator is an IT specialist that is responsible for operating system installation, configuration, patching, user management, monitoring, data backup, implementation of security controls, disaster recovery, and testing.

3. What will happen if you join this study?

If you agree to be in this study, you will be asked to complete a short pre-workshop survey, participate in a 2-hour UNIX/Linux focused security workshop, and then execute an exploitation attack of a cloud-based Linux server using tools demonstrated during the workshop. Finally, after the workshop, you will complete a short post-workshop survey. Surveys will be completed via Qualtrics (online). The workshop will be completed online via a secure Zoom meeting on 5/19/2020 from 9-11 AM. The optional cloud-based penetration test will be available online using EDURange in AWS and will be available 5/19/2020 from 11 AM to 4 PM.

How long will you be in the study?

Your total time participating in this study workshop and cyber lab is two to three hours.

4. What happens to data that are collected in the study?

Johns Hopkins and our research partners work to advance science and public health. The data we collect about you are important to this effort. If you join this study, you should understand that you will not own your research data.

How will your data be shared now and in the future?

Sharing data is part of research and may increase what we can learn from each study. Often, data sharing is required as a condition of funding or for publishing study results. It also is needed to allow other researchers to validate study findings and to come up with new ideas.

No identified data will be shared. De-identified data may be shared with research collaborators or publishers of papers.

We will do our best to protect and maintain your data in a safe way. Generally, if we share your data without identifiers (such as your name) no further review and approval by an Institutional Review Board (IRB) is needed. If data are shared with identifiers, further IRB review and approval may be needed. The IRB will determine whether additional consent is required.

5. What are the risks or discomforts of the study?

This research study involves minimal risk to you. To the best of our knowledge, the things you will be doing have no more risk of harm than you would have in everyday life. You may get tired or bored when we you are completing the survey. You do not have to answer any question you do not want to answer.

6. Are there benefits to being in the study?

We hope the information learned from this study will help increase your

knowledge and awareness of the security threats facing our organization and how best to test, evaluate, and secure your UNIX/Linux servers. There is no guarantee or promise, however, that you will receive any benefit from this study.

7. What are your options if you do not want to be in the study?

If you do not join, your employment/education at Johns Hopkins will not be affected.

8. Can you leave the study early?

You can agree to be in the study now and change your mind later. If you wish to stop, please tell us right away. Leaving the study early will not affect your employment/education. If you leave the study early, Johns Hopkins may use or share your information that it has already collected if the information is needed for this study or any follow-up activities.

9. How will your privacy be maintained and how will the confidentiality of your data be protected?

We try to make sure that everyone who sees your information keeps it confidential, but we cannot guarantee that your information will not be shared with others. Only the principal investigator will have access to any identifying data and that data will not be shared with anyone in the organization.

Do you have to sign this Authorization?

You do not have to sign this Authorization, but if you do not, you may not join the study.

How long will your information be used or shared?

Your Authorization for the collection, use, and sharing of your information

does not expire.

What if you change your mind?

You may change your mind and cancel this Authorization at any time. If you cancel, you must contact the Principal Investigator in writing to let them know by using the contact information provided in this consent form. Your cancellation will not affect information already collected in the study, or information that has already been shared with others before you cancelled your authorization.

How will your information be protected?

Information we learn about you in this research study will be handled in a confidential manner. All responses will be collected in Qualtrics and stored offline at the conclusion of the collection period. This data will be available to the principal investigator, and the Institutional Review Board. If we publish the results of the study in a scientific journal or book, we will not identify you. All data will be kept for 36 months from the end of the study and destroyed after that time.

10. What does a conflict of interest mean to you as a participant in this study?

The researcher running this study is doing this research in partial fulfillment of the requirements for the degree of Doctor of Philosophy in Information Systems. The researcher is not, in any way, gaining financially from this research study.

If you have any questions about this financial interest, please call the Office of Policy Coordination 410-361-8667 for more information. The Office of Policy Coordination reviews financial interests of researchers and/or Johns Hopkins.

11. What other things should you know about this research study?

During the study, we will tell you if we learn any new information that might

affect whether you wish to continue to participate.

What is the Institutional Review Board (IRB) and how does it protect you?

This study has been reviewed by an Institutional Review Board (IRB), a group of people that reviews human research studies. The IRB can help you if you have questions about your rights as a research participant or if you have other questions, concerns, or complaints about this research study. You may contact the IRB at 410-502-2092 or jhmeirb@jhmi.edu. Please refer to JHH Application No.: IRB00240988. The Nova Southeastern University Institutional Review Board can be reached toll free at: 1-866-499-0790 or IRB@nova.edu. Please refer to NSU Application No.: 2020-60

What should you do if you have questions about the study, or are injured or ill as a result of being in this study?

Call or email the principal investigator, John McConnell at 410-935-5657 or jmconn3@jhmi.edu. If you cannot reach the principal investigator or wish to talk to someone else, call the IRB office at 410-502-2092.

12. What does your consent mean?

Your selecting “I consent to participate in this study” means that you have reviewed the information in this form, and you agree to join the study. You will not give up any legal rights by signing this consent form.

I consent and will participate in this study.

I do not consent and will NOT participate in this study.

References

- Acquisti, A. (2004). *Privacy in electronic commerce and the economics of immediate gratification*. Proceedings of the 5th ACM Conference on Electronic Commerce, New York, 21-29.
- Ajami, S., & Bagheri-Tadi, T. (2013). Barriers for adopting electronic health records (EHRs) by physicians. *Acta Informatica Medica*, 21(2), 129-134.
- Albrechtsen, E., & Hovden, J. (2010). Improving information security awareness and behavior through dialogue, participation, and collective reflection. An intervention study. *Computers & Security*, 29(4), 432-445.
- Amarasingham, R., Plantinga, L., Diener-West, M., Gaskin, D. J., & Powe, N. R. (2009). Clinical information technologies and inpatient outcomes: A multiple hospital study. *Architecture and Internal Medicine*, 169(2), 108-114.
- Asadoorian, P. (2010). The value of credentialed vulnerability scanning. Retrieved from: <https://www.tenable.com/blog/the-value-of-credentialed-vulnerability-scanning>.
- Avancha, S., Baxi, A., & Kotz, D. (2012). Privacy in mobile technology for personal healthcare. *ACM Computing Surveys*, 45(1), 3:1-3:54.
- Bagozzi, R. P., & Yi, Y. (1988). On the evaluation of structural equation models. *Journal of the Academy of Marketing Science*, 16(1), 74-94.
- Bajgoric, N. (2006). Information technologies for business continuity: An implementation framework. *Information Management & Computer Security*, 14(5), 450-466.
- Bauer, S., & Bernroider, E. W. N. (2017). From information security awareness to reasoned compliant action: Analyzing information security policy compliance in a large banking organization. *Database for Advances in Information Systems*, 48(3), 44-68.
- Bauer, S., Bernroider, E. W., & Chudzikowski, K. (2017). Prevention is better than cure! Designing information security awareness programs to overcome users' non-compliance with information security policies in banks. *Computers & Security*, 68, 145-159.
- Bélanger, F., Collignon, S., Enget, K., & Negangard, E. (2017). Determinants of early conformance with information security policies. *Information & Management*, 54(7), 887-901.
- Belsis, P., Kokolakis, S., & Kiountouzis, E. (2005). Information systems security from a knowledge management perspective. *Information Management & Computer Security*, 31(3), 189-202.

- Beuchelt, G. (2017a). Securing Web applications, services, and servers. In J.R. Vacca (Ed.), *Computer and information security handbook* (3rd, pp. 183-203). Boston, MA: Morgan Kaufmann.
- Beuchelt, G. (2017b). UNIX and Linux security. In J.R. Vacca (Ed.), *Computer and information security handbook* (3rd, pp. 205-224). Boston, MA: Morgan Kaufmann.
- Blythe, J. M., Coventry, L., & Little, L. (2015). *Unpacking security policy compliance: The motivators and barriers of employees' security behaviors*. Proceedings of the USENIX Symposium on Usable Privacy and Security, Ottawa, CA, 103-122.
- Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., & Polak, P. (2015). What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. *MIS Quarterly*, 39(4), 837-864.
- Brotby, W. K., & Hinson, G. (2013). *PRAGMATIC security metrics: Applying metametrics to information security*. Boca Raton, FL: CRC Press.
- Brotherston, L., & Berlin, A. (2017). *Defensive security handbook*. Boston, MA: O'Reilly.
- Burns, A. J., Roberts, T. L., Posey, C., Bennett, R. J., & Courtney, J. F. (2015). *Assessing the role of security education, training, and awareness on insiders' security related behavior: An expectancy theory approach*. Proceedings of the IEEE 48th Hawaii International Conference on Systems Sciences, HI. Doi:10.1109/HICSS.2015.471.
- Caballero, A. (2013). Information security essentials for IT managers: Protecting mission-critical systems. In J.R. Vacca (Ed.), *Computer and information security handbook* (3rd ed, pp. 391-419). Boston, MA: Morgan Kaufmann.
- Carlton, M., & Levy, Y. (2015). *Expert assessment of the top platform independent cybersecurity skills for non-IT professionals*. Proceedings of the IEEE Southeast Con, Fort Lauderdale, FL. doi: 10.1109/SECON.2015.7132932.
- Chen, X., Chen, L., & Wu, D. (2018). Factors that influence employees' security policy compliance: An awareness-motivation-capability perspective. *Journal of Computer Information Systems*, 58(4), 312-324.
- Cloud Market. (2020, October 11). EC2 statistics: Total images available. Retrieved from <https://thecloudmarket.com/stats>.
- Colwill, C. (2009). Human factors in information security: The insider threat—who can you trust these days? *Information Security Technical Report*, 14(4), 186-196.

- Committee on National Standards. (2010). *National information assurance glossary*. (CNSS instruction no. 4009). Retrieved from <https://www.hsdl.org/?view&did=7447>.
- Connelly, C. E., & Zweig, D. (2015). How perpetrators and targets construe knowledge hiding in organizations. *European Journal of Work and Organizational Psychology*, 24(3), 479-489.
- Cram, W. A., Proudfoot, J. G. & D'Arcy, J. (2017) Organizational information security policies: A review and research framework. *European Journal of Information Systems*, 26(6), 605-641.
- Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. *Computers & Security*, 32(C), 90-101.
- CVE Details. (2020, January 11). Top 50 products by total number of “distinct” vulnerabilities. Retrieved from <https://www.cvedetails.com/top-50-products.php>.
- Dang-Pham, D., Pittayachawan, S., & Bruno, V. (2016). Exploring behavioral information security networks in an organizational context: An empirical case study. *Journal of Information Security and Applications*, 34(1), 46-62.
- Dang-Pham, D., Pittayachawan, S., & Bruno, V. (2017). Why employees share information security advice? Exploring the contributing factors and structural patterns of security advice sharing in the workplace. *Computers in Human Behavior*, 67, 196-206.
- D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research*, 20(1), 79-98.
- D'Arcy, J., & Lowry, P. B. (2019). Cognitive-affective drivers of employees' daily compliance with information security policies: A multilevel longitudinal study. *Information Systems Journal*, 29(1), 43-69.
- Dey, T., & Mukhopadhyay, S. (2018). Influence of behavioral intentions, affective trust and affective commitment on knowledge sharing behavior. *International Journal of Knowledge Management*, 14(2), 37-51.
- Dismukes, K., Berman, B. A., & Loukopoulos, D. (2007). *The limits of expertise: Rethinking pilot error and the causes of airline accidents*. New York, NY: Routledge.

- Dixon, B. E. (2016). What is health information exchange? In B.E. Dixon (Ed.), *Health information exchange: Navigating and managing a network of health information systems*. Boston, MA: Academic Press.
- Donaldson, S. E., Siegel, S. G., Williams, C. K., & Aslam, A. (2015). Building an effective defense. In *Enterprise cybersecurity: How to build a successful cyberdefense program against advanced threats* (pp. 133-156). New York, NY: Springer.
- EDURange. (2019). Scenarios. Retrieved from <https://edurange.org/scenarios.html>.
- Egleman, S., & Peer, E. (2015). *Scaling the security wall: Developing a security behavior intentions scale (SeBIS)*. Proceedings of the CHI Conference, 2015, Seoul, Korea, 2873-2882.
- Epic. (2018). Epic operating system settings and security setup and support guide. Retrieved from https://galaxy.epic.com/?#Browse/page=1!68!50!2220559_
- Epstein, S. (2014). *Cognitive-experiential theory: An integrative theory of personality*. New York, NY: Oxford University Press.
- Fashoto, S., Adabara, I., & Opeyemi, O. G. (2018). Evaluation of network and system security using penetration testing in a simulation environment. *GESJ: Computer Science and Telecommunications*, 2(54), 91-99.
- Ferreira, M. B, Garcia-Marques, L., Sherman, S. J., & Sherman, J. W. (2006). Automatic and controlled components of judgment and decision making. *Journal of Personality and Social Psychology*, 91(5), 797-813.
- Finucane, M. L., Alhakami, A., Slovic, P., & Johnson, S. M. (2000). The affect heuristic in judgment of risks and benefits. *Journal of Behavioral Decision Making*, 13(1), 1-17.
- First.org. (n.d.). Common vulnerability scoring system v3.0: Specification document. Retrieved from <https://www.first.org/cvss/v3.0/specification-document>.
- Fischer, P., Kastenmüller, A., Greitemeyer, T., Fischer, J., Frey, D., & Crelley, D. (2011). Threat and selective exposure: The moderating role of threat and decision context on confirmatory information search after decisions. *Journal of Experimental Psychology: General*, 140(1), 51-62.
- Flores, W. R., Antonsen, E., & Ekstedt, M. (2014). Information security knowledge sharing in organizations: Investigating the effect of behavioral information security governance and national culture. *Computers & Security*, 43, 90-110.

- Furnell, S., & Clarke, N. (2012). Power to the people? The evolving recognition of human aspects of security. *Computers & Security*, 31(8), 983-988.
- Gardner, B., & Thomas, V. (2014). *Building an information security awareness program: Defending against social engineering and technical threats*. New York, NY: Elsevier.
- Gertner, A., Zaromb, F., Roberts, R. D., & Matthews, G. (2016). *The assessment of biases in cognition* (MITRE Technical Report, Case Number 16-0956). Retrieved from <https://www.mitre.org/sites/default/files/publications/pr-16-0956-the-assessment-of-biases-in-cognition.pdf>.
- Gilovich, T., & Griffin, D. (2013). Introduction – heuristics and biases: Then and now. In T. Gilovich, D. Griffin, & D. Kahneman (Eds.), *Heuristics and biases: The psychology of intuitive judgment* (pp. 1-18). New York, NY: Cambridge University Press.
- Gorbacheva, E., Beekhuyzen, J., vom Brock, J., & Becker, J. (2019). Directions for research on gender imbalance in the IT profession. *European Journal of Information Systems*, 28(1), 43-67.
- Gothard, B., Mignot, P., Offer, M., & Ruff, M. (2001). *Career guidance in context*. Thousand Oaks, CA: SAGE.
- Guo, K. H., Yuan, Y., Archer, N. P., & Connelly, C. E. (2011). Understanding nonmalicious security violations in the workplace: A composite behavior model. *Journal of Management Information Systems*, 28(2), 203-236.
- Haber, M., J., & Hibbert, B. (2018). *Asset attack vectors: Building effective vulnerability management strategies to protect organizations*. New York, NY: Springer.
- Hair, J. F., Hult, G. T. M., Ringle, C. M., & Sarstedt, M. (2017). *A primer on partial least squares structural equation modeling (PLS-SEM)*. Thousand Oaks, CA: SAGE.
- Hanus, B., & Wu, Y. (2016). Impact of users' security awareness on desktop security behavior: A protection motivation theory perspective. *Information Systems Management*, 33(1), 2-16.
- Hayden, L. (2010). *IT security metrics: A practical framework for measuring security & protecting data*. New York, NY: McGraw Hill.
- Helms, J., Salazar, B., Scheibel, P., Engels, M., & Reiger, C. (2017). *Safe active scanning for energy delivery systems final report* (Rep. No. LLNL-TR-740556). Livermore, CA: Lawrence Livermore National Lab.

- Henseler, J., Hubona, G., & Ray, P.-A. (2016). Using PLS path modeling in new technology research: updated guidelines. *Industrial Management & Data Systems*, 116(1), 2-20.
- Henseler, J., Ringle, C. M., & Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modeling. *Journal of the Academy of Marketing Science*, 43(1), 115-135.
- Herold, R. (2011). *Managing an information security and privacy awareness and training program* (2nd ed.). Boca Raton, FL: CRC Press.
- HIPAA Journal (2020). Summary of 2019 HIPAA fines and settlements. Retrieved from <https://www.hipaajournal.com/hipaa-enforcement-in-2019/>.
- Hubbard, D. W., & Seirsén, R. (2016). *How to measure anything in cybersecurity risk*. Hoboken, NJ: John Wiley & Sons.
- Hussain, S., Bahadur, F., Gul, F., Iqbal, A., Ashraf, G., & Nazeer, S. (2015). Survey of Windows and Linux as server operating system. *International Journal of Computer*, 18(1), 1-6.
- Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security*, 31(1), 83-95.
- Ifinedo, P. (2014). Information systems security policy compliance: An empirical study of the effects of socialization, influence, and cognition. *Information & Management*, 51(1), 69-79.
- Inshanally, P. (2018). *CompTIA Linux+ certification guide*. Birmingham, UK: Packt.
- Jaquith, A. (2007). *Security metrics: Replacing fear, uncertainty, and doubt*. Boston, MA: Pearson Education.
- Jetty, S., & Rahalkar, S. (2019). *Securing network infrastructure: Discover practical network security with Nmap and Nessus*. Birmingham, UK: Packt.
- Johnston, A. C., Warkentin, M., & Siponen, M. (2015). An enhanced fear appeal rhetorical framework: Leveraging threats to the human asset through sanctioning rhetoric. *MIS Quarterly*, 39(1), 113-134.
- Kahneman, D. (2003). A perspective on judgment and choice: Mapping bounded rationality. *American Psychologist*, 58(9), 697-720.
- Kahneman, D. (2011). *Thinking, fast and slow*. New York, NY: Farrar, Straus, and Giroux.

- Ki-Aries, D., & Faily, S. (2017). Persona-centered information security awareness. *Computers & Security*, 70, 663-674.
- Kliger, D., & Kudryavtsev, A. (2010). The availability heuristic and investors' reaction to company-specific events. *Journal of Behavioral Finance*, 11(1), 50-65.
- Koch, D. D. (2017). Is the HIPAA security rule enough to protect electronic personal health information (PHI) in the cyber age? *Journal of Health Care Finance*, 43(3), 1-32.
- Kraemer, S., & Carayon, P. (2007). Human errors and violations in computer and information security: The viewpoint of network administrators and security specialists. *Applied Ergonomics*, 38(2), 143-154.
- Lowry, P. B., & Moody, G. D. (2015). Proposing the control-reactance compliance model (CRCM) to explain opposing motivations to comply with organizational information security policies: An empirical study of the influence of counterfactual reasoning and organizational trust. *Information Systems Journal*, 25(5), 193-230.
- Marsh, B., Todd, P. M., & Gigerenzer, G. (2004). Cognitive heuristics: Reasoning the fast and frugal way. In J. P. Leighton & R. J. Sternberg (Eds.), *The nature of reasoning* (pp 273-287). Cambridge, UK: Cambridge University Press.
- McFarland, M. (2012). Privacy and the law. *Markkula Center for Applied Ethics at St. Clara University*. Retrieved from <https://www.scu.edu/ethics/focus-areas/internet-ethics/resources/privacy-and-the-law/>
- Meyers, M., & Jernigan, S. (2018). *CompTIA security+ certification guide* (2nd ed.). New York, NY: McGraw Hill.
- MITRE. (2019). CWE-79: *Improper neutralization of input during Web page generation (Cross-site Scripting)*. Retrieved from <https://cwe.mitre.org/data/definitions/79.html>.
- Moqbel, M. A., & Bartelt, V. L. (2015). Consumer acceptance of personal cloud: Integrating trust and risk with the technology acceptance model. *AIS Transactions of Replication Research*, 1, 1-11.
- Newman, D. (2019). Top EHR vendors 2019 – Epic, Cerner, Meditech, Allscripts. *Healthcare IT Skills*. Retrieved from <https://healthcareitskills.com/top-ehr-vendors-allscripts-athenahealth-cerner-epic-meditech/>.

- Ng, B., Kankanhalli, A., & Xu, Y. (2009). Studying users' computer security behavior: A health belief perspective. *Decision Support Systems*, 46(4), 815-825.
- NIST. (n.d.). National Vulnerability Database: NVD Dashboard. Retrieved from <https://nvd.nist.gov/general/nvd-dashboard>.
- Nmap.org. (2019). Nmap: The network mapper. Retrieved September 10, 2020, from <https://nmap.org/>.
- Office of the National Coordinator for Health Information Technology. (n.d.). Federal Health IT Strategic Plan: 2015-2020. Retrieved from <https://dashboard.healthit.gov/strategic-plan/federal-health-it-strategic-plan-2015-2020.php>
- Olsik, J. (2017). The life and times of cybersecurity professionals. *2017 ESG & ISSA Research Report*. Retrieved from <https://www.esg-global.com/esg-issa-research-report-2017>.
- Oparaocha, G.O. (2016). Towards building internal social network architecture that drives innovation: A social exchange theory perspective. *Journal of Knowledge Management*, 20(3), 534-556.
- OWASP. (2017). Deserialization of untrusted data. Retrieved from https://www.owasp.org/index.php/Deserialization_of_untrusted_data.
- Pachur, T., Hertwig, R., & Steinmann, F. (2012). How do people judge risks: Availability heuristic, affect heuristic, or both? *Journal of Experimental Psychology: Applied*, 18(3), 314-330. doi: 10.1037/a0028279.
- Pennycook, G., Trippas, D., Handley, S. J., & Thompson, V. A. (2013). Base rates: Both neglected and intuitive. *Journal of Experimental Psychology*, 40(2), 544-554.
- Pfleeger, S., L., & Caputo, D. D. (2012). Leveraging behavioral science to mitigate cyber security risk. *Computers & Security*, 31(4), 597-611.
- Ponemon Institute. (2019). 2019 Cost of data breach report. Retrieved from <https://www.ibm.com/security/data-breach>.
- Posey, C., Roberts, T., & Lowry, P. B. (2015). The impact of organizational commitment on insiders' motivation to protect organizational information assets. *Journal of Management Information Systems*, 32(4), 179-214.
- Privacy Rights Clearinghouse. (n.d.). Data Breaches. Retrieved from <https://www.privacyrights.org/data-breaches>.

- Rapid7. (n.d.). Metasploitable 2 exploitability guide. Retrieved from <https://metasploit.help.rapid7.com/docs/metasploitable-2-exploitability-guide>.
- Razmerita, L., Kirchner, K., & Nielsen, P. (2016). What factors influence knowledge sharing in organizations? A social dilemma perspective on social media communication. *Journal of Knowledge Management*, 20(6), 1225-1246.
- Redmiles, E., Acar, Y., Fahl, S., & Mazurek, M. (2017). A summary of survey methodology best practices for security and privacy researchers. Retrieved from <https://drum.lib.umd.edu/handle/1903/19227>.
- Renaud, K. (2012). Blaming noncompliance is too convenient: What really causes information breaches? *IEEE Security & Privacy*, 10(3), 57-63.
- Rhee, H., Ryu, Y. U., & Kim, C. (2012). Unrealistic optimism on information security management. *Computers & Security*, 31(2), 221-232.
- Ritchie, D. M., & Thompson, K. (1978). The UNIX time-sharing system. *Bell System Technical Journal*, 57(6), 1905-1929.
- Roberts, M. J. (2004). Heuristics and reasoning I: Making deduction simple. In J. P. Leighton & R. J. Sternberg (Eds.), *The nature of reasoning* (pp 234-272). Cambridge, UK: Cambridge University Press.
- Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *Journal of Psychology*, 91(1), 93-114.
- Rogers, R. W., & Prentice-Dunn, S. (1997). Protection motivation theory. In D.S. Gochman (Ed.), *Handbook of health behavior research I: Personal and social determinants* (pp. 113-132). New York, NY: Plenum Press.
- Rutten, W., Blaas-Franken, J., & Martin, H. (2016). The impact of (low) trust on knowledge sharing. *Journal of Knowledge Management*, 20(2), 199-214.
- Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A., & Herawan, T. (2015). Information security conscious care behavior formation in organizations. *Computers & Security*, 53, 65-78.
- Safa, N. S., & Von Solms, R. (2016). An information security knowledge sharing model in organizations. *Computers in Human Behavior*, 57(C), 442-451.
- Safa, N. S., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model in organizations. *Computers & Security*, 56, 70-82.

- Samtani, S., Yu, S., Zhu, H., Patton, M., & Chen, H. (2016). *Identifying SCADA vulnerabilities using passive and active vulnerability assessment techniques*. Proceedings of the 2016 IEEE Conference on Intelligence and Security Informatics, Tucson, AZ.
- Santara, M. (2013). Eliminating the security weaknesses of linux and UNIX operating systems. In J.R. Vacca (Ed.), *Computer and information security handbook* (3rd ed, pp. 225-238). Boston, MA: Morgan Kaufmann.
- Schroeder, J. (2017). *Advanced persistent training: Take your security awareness program to the next level*. New York, NY: Springer.
- Sedighi, M., van Splunter, S., Brazier, F., van Beers, C., & Lukosch, S. (2016). Exploration of multi-layered knowledge sharing participation: The roles of perceived benefits and costs. *Journal of Knowledge Management*, 20(6), 1247-1267.
- Sekaran, U., & Bougie, R. (2013). *Research methods for business*. West Sussex, UK: John Wiley & Sons.
- Shrivastava, A. (2018). Top 10 EMR software companies in 2018. Retrieved from <https://arkenea.com/blog/top-10-emr-software-companies-in-2018/>.
- Siponen, M., Mahmood, M. A., & Pahlila, S. (2014). Employees' adherence to information security policy: An exploratory field study. *Information & Management*, 51(2), 217-224.
- Siponen, M., Pahlila, S., & Mahmood, M. A. (2010). Compliance with information security policies: An empirical investigation. *IEEE Computer*, 43(2), 64-71.
- SmartPLS.com. (n.d.). Multigroup Analysis. Retrieved from: <https://www.smartpls.com/documentation/algorithms-and-techniques/multigroup-analysis>.
- Steinbrook, R. (2009). Health care and the American Recovery and Reinvestment Act. *New England Journal of Medicine*, 360(11), 1057-1060.
- Sternberg, R. J. (2004). What do we know about the nature of reasoning? In J. P. Leighton & R. J. Sternberg (Eds.), *The nature of reasoning* (pp. 433-455). New York, NY: Cambridge University Press.
- Tenable. (2019). Nessus 8.5.x user guide. Retrieved from: https://docs.tenable.com/nessus/8_5/Content/GettingStarted.htm.
- Terrell, S. (2012). *Statistics translated: A step-by-step guide to analyzing and interpreting data*. New York, NY: Guilford Press.

- Terrell, S. (2016). *Writing a proposal for your dissertation: Guidelines and examples*. New York, NY: Guilford Press.
- Thieme, E. (2016). Privacy, security, and confidentiality: Toward trust. In B.E. Dixon (Ed.), *Health information exchange: Navigating and managing a network of health information systems* (pp. 91-104). Boston, MA: Academic Press.
- Toplak, M. E., West, R. F., & Stanovich, K. E. (2011). The cognitive reflection test as a predictor on heuristics-and-biases tasks. *Memory & Cognition* 39(7), 1275-1289.
- Tsohou, A., Karyda, M., & Kokolakis, S. (2015). Analyzing the role of cognitive and cultural biases in the internalization of information security policies: Recommendations for information security awareness programs. *Computers & Security*, 52, 128-141.
- Tversky, A., & Kahneman, D. (1974). Judgment under uncertainty: Heuristics and biases. *Science*, 185(4157), 1124-1131.
- U.S. Department of Health and Human Services. (2013). Summary of the HIPAA security rule. Retrieved from <https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html>.
- U.S. Department of Health and Human Services Office for Civil Rights. (2020). Breach portal: Notice to the secretary of HHS breach of unsecured protected health information. Retrieved from https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf.
- Vance, A., Siponen, M., & Pahlila, S. (2012). Motivating IS security compliance: Insights from Protection Motivation Theory. *Information & Management*, 49(3-4), 190-198.
- Van Vuuren, I. E. (2016). IT security trust model – securing the human perimeter. *International Journal of Social Science and Humanity*, 6(11), 852-858.
- Vaughan-Nichols, S. J. (2018). Linux now dominates Azure. Retrieved from <https://www.zdnet.com/article/linux-now-dominates-azure/>.
- Verizon. (2019). Verizon data breach investigations report. Retrieved from <https://enterprise.verizon.com/en-gb/resources/reports/dbir/>.
- W3Techs. (2020, October 11). Usage of operating systems for websites. Retrieved from https://w3techs.com/technologies/overview/operating_system/all.
- Wash, R., & Cooper, M. M. (2018). *Who provides phishing training? Facts, stories, and people like me*. Proceedings of the CHI Conference, 2018, Montreal, CA.

West, R. F., Meserve, R. J., & Stanovich, K. E. (2012). Cognitive sophistication does not attenuate the bias blind spot. *Journal of Personality and Social Psychology*, 103(3), 506-519.

Whitman, M. E., & Mattord, H. J. (2012). *Principles of information security* (4th ed.). Boston, MA: Course Technology.

Yoo, C. W., Sanders, G. L., & Cerveney, R. P. (2018). Exploring the influence of flow and psychological ownership on security education, training, and awareness effectiveness and security compliance. *Decision Support Systems*, 108, 107-118.