

University of Texas Rio Grande Valley

**ScholarWorks @ UTRGV**

---

Theses and Dissertations

---

5-2023

## The Effect of Cybersecurity Training on Government Employee's Knowledge of Cybersecurity Issues and Practices

Juan Jaime Saldana II

*The University of Texas Rio Grande Valley*

Follow this and additional works at: <https://scholarworks.utrgv.edu/etd>



Part of the [Curriculum and Instruction Commons](#), and the [Information Security Commons](#)

---

### Recommended Citation

Saldana, Juan Jaime II, "The Effect of Cybersecurity Training on Government Employee's Knowledge of Cybersecurity Issues and Practices" (2023). *Theses and Dissertations*. 1253.

<https://scholarworks.utrgv.edu/etd/1253>

This Dissertation is brought to you for free and open access by ScholarWorks @ UTRGV. It has been accepted for inclusion in Theses and Dissertations by an authorized administrator of ScholarWorks @ UTRGV. For more information, please contact [justin.white@utrgv.edu](mailto:justin.white@utrgv.edu), [william.flores01@utrgv.edu](mailto:william.flores01@utrgv.edu).

THE EFFECT OF CYBERSECURITY TRAINING ON GOVERNMENT  
EMPLOYEE'S KNOWLEDGE OF CYBERSECURITY  
ISSUES AND PRACTICES

A Dissertation

by

JUAN JAIME SALDANA II

Submitted in Partial Fulfillment of the  
Requirements for the Degree of  
DOCTOR OF EDUCATION

Major Subject: Curriculum and Instruction

The University of Texas Rio Grande Valley

May 2023



THE EFFECT OF CYBERSECURITY TRAINING ON GOVERNMENT  
EMPLOYEE'S KNOWLEDGE OF CYBERSECURITY  
ISSUES AND PRACTICES

A Dissertation  
by  
JUAN JAIME SALDANA II

COMMITTEE MEMBERS

Dr. Joseph Rene Corbeil  
Chair of Committee

Dr. Maria Elena Valdes-Corbeil  
Committee Member

Dr. Zhidong Zhang  
Committee Member

May 2023



Copyright 2023 Juan Jaime Saldana II  
All Rights Reserved



## ABSTRACT

Saldana II, Juan J., The Effect of Cybersecurity Training on Government Employee's Knowledge of Cybersecurity Issues and Practices. Doctor of Education (Ed.D.), May, 2023, 135 pp., 21 tables, 18 figures, references, 66 titles.

There is an ever-pressing need for cybersecurity awareness and implementation of learning strategies in the workplace to mitigate the increased threat posed by cyber-attacks and exacerbated by an untrained workforce. The lack of cybersecurity knowledge amongst government employees has increased to critical levels due to the amount of sensitive information their agencies are responsible for. The digital compromise of a government entity often leads to a compromise of constituent data along with the disruption of public services (Axelrod, 2019; Yazdanpanahi, 2021). The need for awareness is further complicated by agencies looking to cater to a digital culture looking for a balance in government transparency and access by providing more services online. This act of modernizing services for a connected constituency adds further risk to the agency by exposing its workforce to threats associated with the internet-connected world. If their workforce is not prepared for the tactics used by cybercriminals, the consequences can be both fiscally and politically reprehensible. This study considers the knowledge enhancements resulting from the incorporation of cybersecurity training for local government employees in South Texas and the potential effects it will have on the cybersecurity awareness of the population. This study requires the



collection and analysis of the following archival data: the results of a state-mandated cybersecurity awareness training and Cybersecurity Awareness Survey, which was adapted from the Pew Research Center's (2016) Cybersecurity Knowledge Quiz. The purpose of this study is to analyze the effect of a cybersecurity awareness training program on government employees' knowledge of cybersecurity issues and their ability to mitigate cybersecurity threats.

*Keywords:* Breach, Cryptovirology, cybersecurity, exploit, firewall, malware, mitigation, NIST framework, ransomware, threat actors



## DEDICATION

This dissertation is dedicated to all the mentors I've had over the years that saw in me that which I did not. Those mentors gave me the courage to continue my education to a level that I never thought possible. People like Mr. Valdes, a Cuban immigrant that through his stories showed me that prosperity comes through hard work, making the American dream achievable. Like Mr. Elizondo who always pressed on the importance of education on me, no sooner was I done with a Master's degree than he pressed for these Doctoral studies, he made me into a lifetime learner. Lastly, the late Mr. Hernandez, was instrumental and supportive when I was first starting my education, when I didn't know if I would be able to make it to school, he made sure that I did. It is mentors like them that often go unnamed or under-recognized, my success is their success.



## ACKNOWLEDGMENTS

I will always be grateful to Dr. Rene Corbeil, my dissertation committee chair, for being there at the start of my graduate studies a decade ago. How the simple decorations in his office were enough to show me that I had found the next step in my educational career, almost as if a sign from above. My thanks and appreciation go to my committee members Dr. Maria Elena Valdes-Corbeil and Dr. Zhidong Zhang, their patience and input were invaluable to the completion of this dissertation.

I would also like to thank the Cameron County Commissioner's Court and Administration for allowing me to conduct my research and add additional value to the work my team and I provide the constituents of Cameron County. I would like to also acknowledge the IT department at Cameron County for being understanding and accepting of the work I was doing.



## TABLE OF CONTENTS

	Page
ABSTRACT.....	iii
DEDICATION.....	v
ACKNOWLEDGMENTS .....	vi
TABLE OF CONTENTS.....	vii
LIST OF TABLES.....	x
LIST OF FIGURES .....	xii
CHAPTER I INTRODUCTION.....	1
Introduction.....	1
Statement of the Problem.....	2
Need for the Study .....	3
Purpose of the Study.....	5
Research Questions .....	9
Research Hypothesis .....	9
Significance of the Study.....	10
Definitions of Terms .....	12
Organization of the Dissertation .....	16
Summary .....	16
CHAPTER II REVIEW OF THE LITERATURE.....	17
Introduction.....	17
An Emerging Cybersecurity Threat .....	18
Conceptual Framework .....	22
Factors Influencing Cybersecurity Awareness .....	26
Cybersecurity education.....	27
Paradigms for Cybersecurity Education.....	27
Education Is Critical To Cybersecurity Awareness.....	29
Improving Employees’ Capacity For Cybersecurity Through Malware Training .....	31

Effectiveness of Training on Cybersecurity Incidents .....	32
Measuring Awareness .....	33
Factors Related to Cybersecurity Awareness .....	34
Cybersecurity Awareness and Knowledge.....	35
Surveying internet usage and cybersecurity awareness .....	36
Improving cybersecurity awareness with data analytics .....	37
Raising cybersecurity awareness .....	38
Cybersecurity Awareness in Government .....	39
Using Phishing to Test Awareness .....	41
Demographic Factors Impacting Cybersecurity .....	42
Gender Differences in Cybersecurity Behaviors .....	43
Adult learners and cybersecurity education .....	44
Education Level and Cybersecurity Confidence .....	45
Industry Perception of Cybersecurity Threat .....	46
Cryptovirology: The Rise of Ransomware .....	46
Understanding The Gap Between Perceived Threats to and Preparedness for Cybersecurity .....	48
Cybersecurity in Local Government .....	49
Motivational Factors Influencing Cybersecurity Intent to Act.....	51
Skills and Successful Cybersecurity Advocacy .....	52
Safer Practices to Enhance Cybersecurity in Government. ....	53
Summary .....	54
<b>CHAPTER III RESEARCH METHODS .....</b>	<b>55</b>
Introduction.....	55
Research Design and Methodological Rationale .....	56
Participants.....	56
Cybersecurity Program .....	59
Instrumentation .....	60
Cybersecurity Knowledge Survey .....	60
Demographics Survey .....	62
Data Collection Procedures.....	64
Data Analysis Procedures .....	65
Limitations of the Study.....	67



Prior Exposure to Cybersecurity Awareness Content .....	67
Phishing Test Data.....	68
Limitations related to one-group quasi-experimental research design with pre-and post-test Research .....	68
Limitations related to survey research.....	68
Limitations related to the Covid-19 pandemic .....	69
Validity and Reliability of the Survey Instrument .....	69
Extraneous Variables .....	69
Summary .....	70
CHAPTER IV RESULTS.....	71
Introduction.....	71
Results Summary .....	72
Results Obtained for Research Hypothesis One.....	72
Results Obtained for Research Hypothesis Two .....	73
Results Obtained for Research Hypothesis Three .....	79
Summary .....	93
CHAPTER V CONCLUSIONS, INTERPRETATIONS, AND IMPLICATIONS .....	94
Introduction.....	94
Conclusion and Interpretation for Hypothesis One .....	95
Conclusion and Interpretation for Hypothesis Two .....	96
Conclusion and Interpretation for Hypothesis Three .....	99
Implications for Research .....	100
Implications for Practice .....	104
Recommendations for Future Research .....	108
Summary .....	110
REFERENCES .....	112
APPENDIX A.....	119
APPENDIX B .....	129
APPENDIX C .....	132
APPENDIX D.....	134
BIOGRAPHICAL SKETCH .....	135



## LIST OF TABLES

	Page
Table 1: Gender and Age.....	57
Table 2: Gender and Education.....	58
Table 3: Descriptive Statistics.....	72
Table 4: Phishing Campaign 2018 .....	74
Table 5: Phishing Campaign 2019 .....	75
Table 6: Phishing Campaign 2021 .....	76
Table 7: Phishing Campaign 2022 .....	77
Table 8: Descriptive Statistics of Pre- and Post-Test Scores by Demographics .....	80
Table 9: ANOVA results from variable intersections .....	81
Table 10: Predictors will be kept in the stepwise model .....	83
Table 11: ANOVA comparison between Age and Post-Test Scores.....	84
Table 12: ANOVA results post-test vs age.....	84
Table 13: Comparison between highest education level attained and post-test score. ....	85
Table 14: Descriptive statistics Education vs. Post-test scores.....	85
Table 15: ANOVA results in posttest vs Highest Education Level Attained. ....	86
Table 16: Post Hoc Test Comparison of Gender .....	86
Table 17: ANOVA results posttest vs Gender.....	87
Table 18: Analysis of Means for Gender.....	87
Table 19: Pairwise comparison between self-assessed technical skills .....	88

Table 20: ANOVA results posttest vs Self-Assessed Skill Level.....	89
Table 21: Descriptive Statistics for Self-Assessed Technical Skills and Post-test Scores .....	89

## LIST OF FIGURES

	Page
Figure 1: What is Social Engineering .....	5
Figure 2: Personal Internet safety .....	6
Figure 3: Is your organization cybersecurity prepared .....	6
Figure 4: Study framework adapted from Sherif <i>et al.</i> (2015)'s conceptual framework for information security culture. ....	23
Figure 5: Paradigms in information assurance/cybersecurity .....	28
Figure 6: Self-Assessed Technical Skills by Gender .....	58
Figure 7: Self-Assessed Technical Skills by Age Group .....	59
Figure 8: Bloom's Taxonomy (Halawi et al. (2009)) .....	61
Figure 9: Analysis of variance across time .....	65
Figure 10: Phishing Campaigns in 2018-2022 with click trend .....	78
Figure 11: Identifying Phishing Techniques .....	90
Figure 12: What is ransomware? .....	91
Figure 13: Secure Passwords .....	92
Figure 14: 2019 Survey question result. ....	97
Figure 15: Pre-test results for ransomware .....	102
Figure 16: Post-test results for ransomware .....	103
Figure 17: Strong Passwords National vs. Cameron County .....	105
Figure 18: MFA identification National vs. Cameron County .....	107



## CHAPTER I

### INTRODUCTION

#### **Introduction**

As a digital society, we live in a connected world inclusive of our personal, professional, and academic lives. Furthermore, digital citizens have certain expectations for their interactions with government agencies. These interactions require that government agencies adopt new technologies to meet the needs of their constituents. However, with technology adoption comes additional risk in the form of cyber-attacks and ransomware. Government agencies now face additional challenges beyond the public and political. The vast amounts of constituent data they collect make them a prime target for cyber-criminals. While technology solutions are available to mitigate cybersecurity issues within an organization, the first line of defense and prevention is a cyber-educated workforce. Cybersecurity awareness has become more important in recent years due to the increased access to the internet, the availability of multiple connected devices, and the advent of digital citizenship.

There are “malicious actors who aim to use social engineering to exploit users into giving up valuable and confidential information” (Diaz *et al.* 2020, p. 44). Cybersecurity awareness training uses cyber education to help mitigate or even prevent data breaches within an organization. Cyber breaches can be among the most devastating events that can occur within an organization, so understanding the effectiveness of cybersecurity training on an employee’s knowledge and of cybersecurity concepts becomes paramount. However, many organizations do

not adopt cybersecurity tools and training until after experiencing a breach, usually with disastrous consequences for the organization and its patrons (Chowdhury *et al.*, 2019). Black *et al.* (2018) further argue that “those who do not have formal training or career experience in cybersecurity struggle with understanding” cybersecurity concepts and therefore put their organizations at risk (p. 1822). Moreover, there are many reports of government agencies being breached or compromised, however, there is also a lack of quantitative research regarding prior steps taken to prepare for and mitigate cyber-attacks (Macmanus *et al.*, 2013; Kweon *et al.*, 2019). This lack of understanding and awareness of cybersecurity concepts can lead to the vast amounts of constituent data collected by government agencies being at risk of being compromised in a cyber-attack.

### **Statement of the Problem**

The lack of knowledge regarding cybersecurity concepts among internet users has become a serious problem, and for government organizations whose employees lack cybersecurity awareness, it has become a critical problem (Diaz *et al.*, 2020; CISA, 2020; Chowdhury *et al.*, 2019). This lack of awareness of cyber threats has facilitated the work of cybercriminals to exploit these individuals and compromise the organizations that employ them. These compromises can be both devastating and life-altering to an individual due to the potential for embarrassment and financial ruin. However, a compromise such as a data breach or ransomware attack at the government level can expose employee and constituent data, affect tens of thousands of individuals, or disrupt services that can lead to millions of dollars in damages. This challenge raises many questions. How does an organization disseminate cybersecurity awareness training when the topics are potentially too complex for the average computer-using employee? Will training employees on complex cybersecurity topics and daily tasks be met with



resistance and lackluster results? Regardless of the answers to these questions, cybersecurity education needs to be seriously considered, especially when “the human factor, or error, is responsible for 95% of security incidents” (Diaz *et al.*, 2020, p. 53). It only takes one employee to make a mistake that can cripple an entire organization, expose sensitive data, or cause millions of dollars in damage and lost productivity. Accordingly, it is in an organization's self-interest to understand the consequences of having an employee base that does not possess basic cybersecurity knowledge to recognize cybercrime tactics. These organizations should “empower employees through a workforce transformation to meet the growing security expectations of the 21st century” (Axelrod, 2019, p. 2). A training program for any organization must consider relevance to work-related tasks, and end-user risk, and provide opportunities to mitigate to create an effective and aware workforce, most importantly it should be part of the solution to the problem and not a hindrance to daily tasks (Miller, 2017). Therefore, a cybersecurity-educated workforce can be an invaluable addition to an organization’s defense against cyber threats.

### **Need for the Study**

Cybersecurity threats are growing in intensity, regularity, and severity and are a threat to the security of the United States. The internet is no longer as safe as its patrons once thought it was; cybercrime is a phenomenon that continues to be of worldwide concern and has only been exacerbated by major events including but not limited to the U.S. Presidential election and the Coronavirus Pandemic (CISA, 2020). Digital citizens live in a completely connected world, which is all-encompassing in their personal and professional lives. The lack of cybersecurity awareness amongst internet users has made it easy for cybercriminals to exploit and compromise the organizations they work for, especially when these company employees are responsible for most cybersecurity-related incidents (Diaz *et al.*, 2020). Yet these organizations often have

difficulty with the application of security-based technology and even more difficulty ensuring that all employees receive cybersecurity education. Bruijn and Janssen (2017) further suggest that while “communication about cybersecurity issues is a difficult endeavour” for organizations, the behavior of their employees does not reflect a sufficient level of awareness, and while “almost everybody has heard of cybersecurity,” and yet “people are often not worried about cybersecurity” (p. 2).

Correspondingly, a lack of cybersecurity knowledge can be correlated to an uptick in what is now known as *cybercrime*, as would-be criminals develop methods to exploit internet users' lack of security and internet safety practices. The lack of proper training and the resultant lack of knowledge suggests that while “cyberspace offers an endless list of services and opportunities,” for these uninitiated users “it is also accompanied by many risks, of which many Internet users are not aware” (Kortjan and Solms, 2014, p. 29). The exploitation of these users and systems suggests that everyone can be a potential threat to the organization. The need for “policies to be in place and that people understand” is required, “as we know that unawareness on the part of users can introduce further vulnerabilities” (Bruijn and Janssen, 2017, p. 4). The use of cybersecurity awareness training as an educational mitigation tool against cyber-attacks requires critical research to determine if the effectiveness of the training on an employee’s level of cybersecurity awareness is sufficient to stay a security breach.

Cormier (2019) agrees that with “the rapid influx of electronics into all aspects of daily life and the constant movement of massive amounts of data, cybersecurity becomes ever more important” (p. 32). People’s lack of cybersecurity knowledge affects not only their personal but their professional lives which can leave their respective employers open to a security compromise. Accordingly, it becomes necessary for organizations to provide their cybersecurity

awareness training to develop a more cyber security-aware workforce to minimize the probability of a compromise on their secured data. Training that is implemented successfully can effectively raise cybersecurity awareness while helping to reduce cybersecurity breaches. This allows more government entities to consider incorporating cybersecurity awareness training as part of their training regimen. Therefore, studying the effects of cybersecurity training on government employees' knowledge of cybersecurity issues and their ability to mitigate cybersecurity threats warrants investigation.

### **Purpose of the Study**

This research study was prompted based on the results of a cybersecurity awareness survey conducted by the Cameron County government, during the internationally observed Cybersecurity Month in the Fall of 2019, which reflected some deficiencies in Cameron County employees' knowledge of common cybersecurity threats. The results of the 2019 survey reflected the current state of cybersecurity awareness within the selected population of government employees. There were some key findings in the survey results listed below and are listed as follows:

- Nearly 39% of the surveyed population had never heard of social engineering.

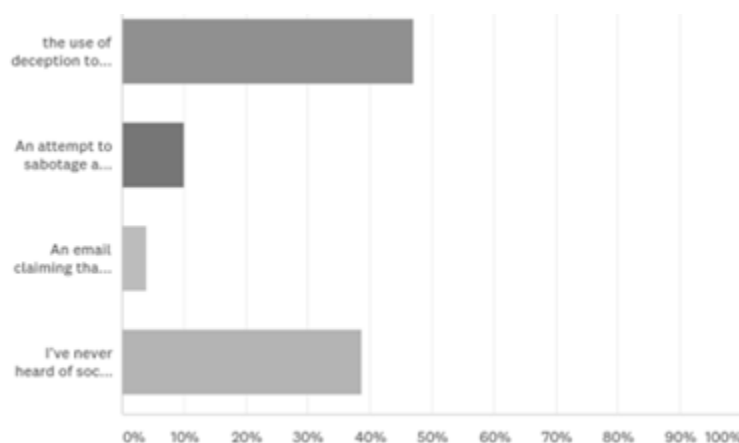


Figure 1: What is Social Engineering

- 55% felt that they were personally vulnerable to cyberattacks, while 6% were not personally concerned with their cybersecurity.

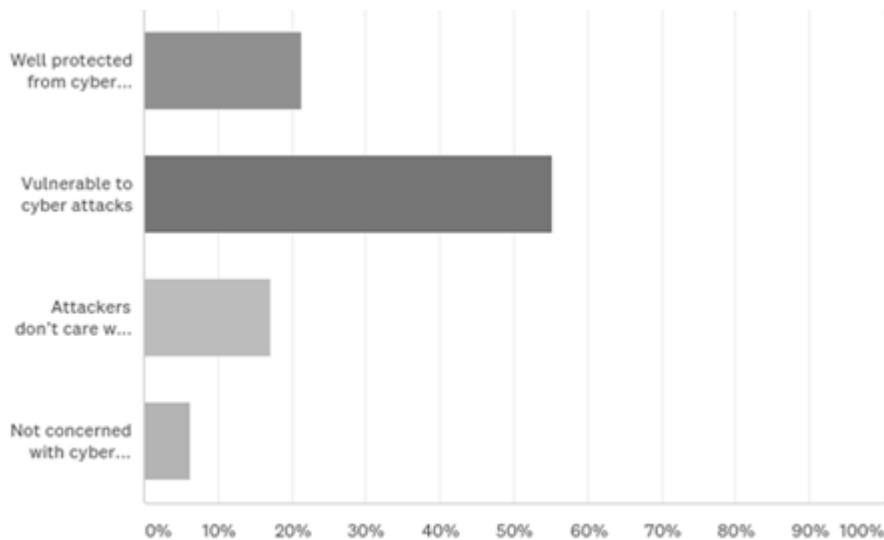


Figure 2: Personal Internet safety

- The most concerning was that a combined 63% believed that their organization was at risk of a cyber-related incident or were indifferent about its cybersecurity preparedness.

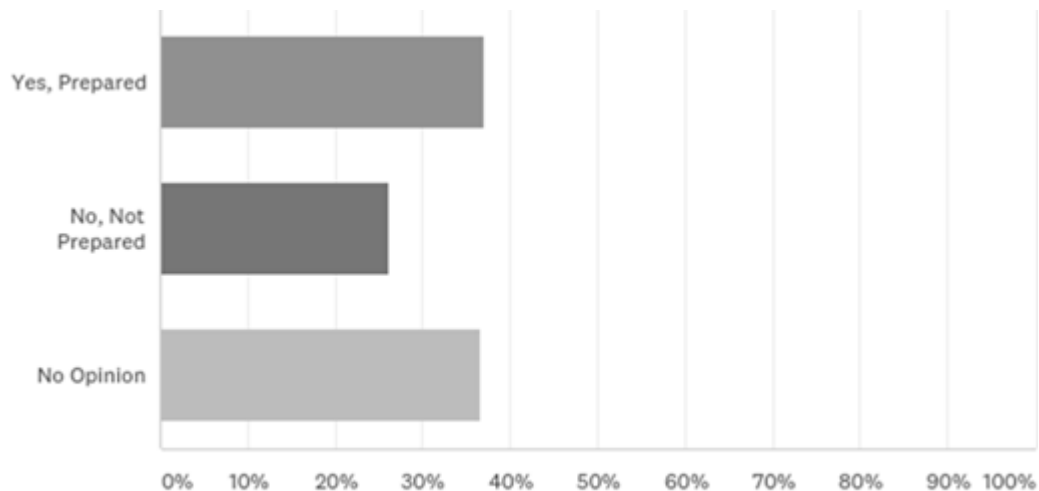


Figure 3: Is your organization cybersecurity prepared

More importantly, the survey also exposed several online behaviors that could be addressed with proper cybersecurity awareness training. The application of proper training and

the resulting knowledge can help internet users be aware of the many risks including but not limited to their use of public Wi-Fi, the adoption of unsecured passwords, and their lack of personal cybersecurity hygiene. There are many ways to combat cybercrime and the provision of adequate training is one way to improve an employee/learner's awareness, which in turn can improve their online safety and the organization's security posture. However, Bruijn and Janssen (2017) argue that "despite all their good intentions and countermeasures, there is always the potential that an organization will suffer a cybersecurity attack" (p. 4).

A digital society is a progressive society that is the result of the adaptation of technology and internet connectivity. A digital government furthers that by adopting several digital tools to meet the requirements of tech-savvy digital citizens looking to conduct their government-related business online. The adoption of internet-based technologies by any organization comes at the cost of ensuring the security of that data, this is especially true of government agencies that are required to safeguard the information of their constituents along with their organizational data. The act of securing digital data is at the core of cybersecurity and is defined by The National Initiative for Cybersecurity Careers and Studies (NICCS) as "any activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation" (NICCS, 2021, Vocabulary).

Securing digital data is easier said than done, as while technology can be used to secure an organization to a certain extent, cybercriminals and modern cybercrime tactics have now started to target the "human firewall" otherwise known as organizational employees (Diaz *et al.*, 2020; Chowdhury *et al.*, 2019). Kemper (2019) furthers that for many organizations, "employees pose the greatest cybersecurity threats" to their corporate data and networks,

especially when they are not trained to be cybersecurity aware (p. 11). Cybercriminals seek to exploit employees who are not aware of these tactics and the only way to mitigate this potential exploit of an organization is through awareness education. In fact, the South Texas government agency where this study's researcher works experienced a virus attack in November of 2017, as a consequence of a user opening an e-mail with a malicious attachment. While the attack was contained and mitigated, it took several days to fully restore operations at that building. These are the kinds of situations that have played out across various locations in the State of Texas at businesses, schools, and government agencies alike. In 2019, to mitigate the growing threat of cybercrime, The Texas House of Representatives in conjunction with the Department of Information Resources (DIR) passed House Bill 3834, which mandated the annual completion of a cybersecurity awareness training course by all State and local government employees that use a computer to conduct at least 25% of their work. The initial piloted training was conducted in the first half of 2020, which served as a benchmark for conducting agency-wide, mandated training. In 2021, the Cameron County Information Technology Department was taking an active role in conducting the training and collecting metrics for the training. Archival data in the form of employees' pre-and post-test scores were collected and will be analyzed in this study. A training platform was purchased to enhance the training with mock phishing attempts and scenarios to enhance the learner experience and engagement. This training will continue to be conducted at regular intervals and on an ongoing basis in an effort to improve the agency's cybersecurity knowledge and awareness, which theoretically could reduce the cyber risk faced by this government agency.

## **Research Questions**

Based on the proposed purpose stated above, this research study has explored the following research questions:

- What is the effect of a cybersecurity awareness training program on government employees' knowledge of cybersecurity issues and practices?
- What is the effect of a cybersecurity awareness training program on government employees' ability to mitigate cybersecurity threats?
- What demographic factors are related to government employees' knowledge of cybersecurity issues and practices and their ability to mitigate cybersecurity threats?

## **Research Hypothesis**

The hypothesis will be proven true if:

- There is a statistically significant positive effect of a cybersecurity awareness training program on government employees' knowledge of cybersecurity issues and practices as measured by a comparison of their pre-and post-test scores.
- There is a statistically significant positive effect of a cybersecurity awareness training program on government employees' ability to mitigate cybersecurity threats as measured by the frequency of mitigated cybersecurity threats identified prior to and after the training
- There is a statistically significant relationship between employees' cybersecurity awareness scores and demographic variables such as gender, age, and the highest level of education attained.

## **Significance of the Study**

The internet was an innovation that made our otherwise massive world's information more accessible to individuals across their multiple connected devices. The internet has changed almost every aspect of our lives, including how society interacts with one another and the way businesses are run. The internet has also changed the rules of modern warfare, how countries can now attack one another without ever firing a single bullet or dropping a single bomb, yet capable of debilitating a rival country's infrastructure. For evidence of this, we only need to research the Solarwinds hack of 2021, which was presumably perpetrated by the Russian threat actors (hackers) and led to the compromise of 12 federal agencies including the U.S. Department of Defense and several major Fortune 500 companies (Jibilian and Canales, 2021). While not all cyber-attacks are related to political and military agendas, most are the result of threat actors who are looking for financial gain as a result of an organization's misfortune. These threat actors are usually malicious groups or individuals responsible for the security incident, which can compromise an organization's security infrastructure. The attacks can cripple an organization's computer network or quietly steal sensitive data such as the personal identification data of an organization's employees or customers without their knowledge. These threats compel many organizations to provide robust cybersecurity training in the hope of developing a workforce more knowledgeable in cybersecurity concepts while lowering the probability of a compromise of their secured data. A data breach or the theft of sensitive or proprietary data by a threat actor can permanently damage an organization's reputation and lower its trust level amongst customers, which is even more critical for a government agency managing constituent data.

The significance of this research is notable in that the findings of this study could contribute to understanding the need for a workforce more knowledgeable in cybersecurity



concepts while helping security practitioners understand the effectiveness of training programs to help facilitate that knowledge. More effective training, based on research data, can be used to improve the existing state of cybersecurity awareness within organizations including but not limited to public, private, and educational institutions. Furthermore, understanding that the human factor in the organization's security posture plays as much of a role as their technical defenses furthers the organizational need for security training of their workforce. As Diaz *et al.* (2020) asserted that "the human factor, or error, is responsible for 95% of security incidents" (p. 53) and affirmed by Chowdhury *et al.* (2019) who similarly stated that "it is estimated that more than 95 percent of successful cyber-attacks are caused by human error" (p. 1290), cybersecurity awareness is becoming more important, especially in recent years due to the increased access to the internet, the availability of multiple connected devices, and the advent of digital citizenship. The need for cybersecurity is evident when most internet users believe that "anti-virus with a firewall is the only requirement for protecting data, privacy, and security" (Tirumala *et al.*, 2016, p. 228). This research can assist policymakers in the identification of security challenges and help in the development of security policies, procedures, and training curricula. This research could also help the perceptions of organizations, who are looking for ways to address the increasing role of cybersecurity knowledge through awareness programs for their employees. It is hoped (or hypothesized) that the more knowledgeable a workforce is about cybersecurity threats, the less likely they will be to fall for the deceptive techniques of cyber criminals. This premise is supported by Costa *et al.* (2019) who proclaimed, "It is vital for the organizations to foster a culture of security and responsibility on users," as they are a functional part of the organization's security posture (p. 2033). To this end, this research has studied the effect of

cybersecurity training on government employees' knowledge of cybersecurity issues and their ability to mitigate cybersecurity threats.

### **Definitions of Terms**

The following terms will be discussed throughout this dissertation and are operationally defined in the context of this research study.

**Cryptovirology.** Young and Yung (2017) define the field of Cryptovirology as the study of how cryptographic technology is used to design powerful malicious software and viruses.

**Cybersecurity.** The term cybersecurity is defined by National Initiative for Cybersecurity Careers and Studies as “any activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation” (NICCS, 2021, Vocabulary).

**Data Breach.** The term breach or more specifically data breach is defined by National Initiative for Cybersecurity Careers and Studies as “the unauthorized movement or disclosure of sensitive information to a party, usually outside the organization, that is not authorized to have or see the information” (NICCS, 2021, Vocabulary).

**Exfiltration.** The term exfiltration or more specifically data exfiltration is defined by the National Initiative for Cybersecurity Careers and Studies as the “unauthorized transfer of information from an information system” (NICCS, 2021, Vocabulary).

**Exploit.** The term exploit is defined by the National Initiative for Cybersecurity Careers and Studies as “any malicious application or script that can be used to take advantage of a

computer's vulnerability" (NICCS, 2021, Vocabulary). A technique to breach the security of a network or information system in violation of security policy.

**Firewall.** The term firewall is defined by the National Initiative for Cybersecurity Careers and Studies as "the capability to limit network traffic between networks and/or information systems. A hardware/software device or a software program that limits network traffic according to a set of rules of what access is and is not allowed or authorized" (NICCS, 2021, Vocabulary).

**Human Firewall.** It is a commitment of a group of employees to follow best practices to prevent as well as report any data breaches or suspicious activity. The more employees you have committed to being a part of the security system, the stronger it gets (Chowdhury *et al.*, 2019; Moramarco, S., 2020).

**Malware.** The term malware is defined by the National Initiative for Cybersecurity Careers and Studies as any "software that compromises the operation of a system by performing an unauthorized function or process" (NICCS, 2021, Vocabulary). A wide variety of types of malware exist, including computer viruses, worms, Trojan horses, ransomware, spyware, adware, rogue software, and scareware.

**Mitigate.** The term mitigate is defined by the National Initiative for Cybersecurity Careers and Studies as "the reduction in severity or seriousness of an event. In cybersecurity, mitigation is centered around strategies to limit the impact of a threat against data in custody" (NICCS, 2021, Vocabulary).

**Multi-Factor Authentication (MFA).**

The term is defined by the Cybersecurity and Infrastructure Security Agency as “a layered approach to securing your online accounts and the data they contain. When you enable MFA in your online services (email, online banking, or social media), you must provide a combination of two or more authenticators to verify your identity before the service grants you access. Using MFA protects your account more than just using a username and password” (CISA, 2020).

**NCSAM.** The term NCSAM is an acronym for Nation Cybersecurity Awareness Month and since 2004, the President of the United States and Congress have declared the month of October to be Cybersecurity Awareness Month. The premise is to bring cybersecurity to the forefront by helping individuals protect themselves from online threats. Due to the increased threat to technology, critical infrastructure, and confidential data have become more commonplace. (CISA, 2020)

**NIST Framework.**

The term NIST Framework is defined by the National Institute of Standards and Technology as “a policy framework of computer security guidance for how private sector organizations in the United States can assess and improve their ability to prevent, detect, and respond to cyber-attacks. It provides a high-level taxonomy of cybersecurity outcomes and a methodology to assess and manage those outcomes” (NIST, 2018).

**Phishing.** A technique for attempting to acquire sensitive data, such as bank account numbers, through a fraudulent solicitation in email or on a website, in which the perpetrator masquerades as a legitimate business or reputable person (NIST, 2018).

**Ransomware.**

The term ransomware is defined by the Cyber Security and Infrastructure Security Agency as “an ever-evolving form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption. Ransomware actors often target and threaten to sell or leak exfiltrated data or authentication information if the ransom is not paid” (CISA, 2020).

**Security Posture.** The security status of an enterprise’s networks, information, and systems are based on information security resources (e.g., people, hardware, software, policies) and capabilities in place to manage the defense of the enterprise and to react as the situation changes. (NIST, 2018).

**Spear-Phishing.** The term Spear phishing is defined by the company KnowBe4 as “the act of sending emails to specific and well-researched targets while purporting to be a trusted sender. The aim is to either infect devices with malware or convince victims to hand over information or money” (KnowBe4, n.d.).

**Social Engineering.** It is defined as when an adversary exploits human traits, such as modesty, altruism, empathy, and diligence of a victim to gain access to restricted resources, steal secrets, or cause other kinds of havoc (Schürmann *et al.*, 2020).

**Threat Agent.** The term threat agent or threat actor is defined by the Cyber Security and Infrastructure Security Agency as “an individual, group, organization, or government that conducts or has the intent to conduct detrimental activities. In threat intelligence, actors are generally categorized as external, internal, or partner” (NICCS, 2021, Vocabulary).

**Threat Mitigation.** The term mitigation is defined by the National Initiative for Cybersecurity Careers and Studies as “the application of one or more measures to reduce the likelihood of an unwanted occurrence and/or lessen its consequences. Implementing appropriate risk-reduction controls based on risk management priorities and analysis of alternatives” (NICCS, 2021, Vocabulary).

### **Organization of the Dissertation**

This dissertation is organized into five chapters. The present chapter, Chapter One, serves as the introduction to the study. This chapter also includes the need for the study, presents a statement of the problem, defines the purpose of the study, presents the hypotheses, and provides definitions of cybersecurity terms. Chapter Two provides a review of the relevant literature, focusing on existing studies discussing cyber-attacks, awareness of cybersecurity concepts, and the benefits of a cybersecurity-knowledgeable workforce. Chapter Three describes the methodology utilized for the study, explaining the concepts behind the research design, participants, instrumentation, treatment, data collection procedures, data analysis procedures, and limitations of the study. Chapter Four presents the results of the study. The last chapter, Chapter Five presents the conclusion to the study, interpretations, and implications from the results obtained while also offering recommendations for future activities.

### **Summary**

This chapter aimed to provide a brief overview of the problem of cybersecurity and its background, including vulnerabilities, especially concerning cybersecurity knowledge and the human factor. The next section will review relevant literature that will further highlight the need for cybersecurity training and the mitigation benefits organizations have seen as a result.

## CHAPTER II

### REVIEW OF THE LITERATURE

#### **Introduction**

The purpose of this study was to analyze the effect of a cybersecurity awareness training program on government employees' knowledge of cybersecurity issues and their ability to mitigate cybersecurity threats and will be explored using the following research questions:

- What is the effect of a cybersecurity awareness training program on government employees' knowledge of cybersecurity issues and practices?
- What is the effect of a cybersecurity awareness training program on government employees' ability to mitigate cybersecurity threats?
- What demographic factors are related to government employees' knowledge of cybersecurity issues and practices and their ability to mitigate cybersecurity threats?

In this chapter, a literature review is offered to provide a synopsis of the relevant cybersecurity literature related to training, management intervention, awareness, intention to act, and the resultant employee behaviors as presented in the theoretical framework adapted for this study. The literature review was a critical part of the development and adaptation of the theoretical framework used for this study. A systematic search of the existing body of knowledge for quality peer-reviewed and cybersecurity-related literature validates the presence

of the research problem while justifying and adding structure to the study. Existing subject matter expert knowledge, research questions, and theoretical underpinning for this study of disseminating and empirically testing a cybersecurity course for an improvement in cybersecurity skills were discovered from this literature review.

### **An Emerging Cybersecurity Threat**

The Internet and its use are a critical part of the daily operations of many organizations in the public, private, and educational business sectors. The same holds for individuals and their use of social media, email, and streaming services along with their exorbitant use of the internet. Research shows that while the use of the internet is increasing, safe practices on the internet, otherwise known as cybersecurity, are not equally increasing (Costa *et al.*, 2019; Chowdhury *et al.*, 2019; and Tirumala *et al.*, 2019). As digital citizens, we conduct financial transactions and freely share personal details, all while children converse with total strangers while gaming online. This new digital reality has led to a new tactic by threat actors, known as social engineering, where criminals use publicly available information tricks users into providing additional and more sensitive information or enacting a compromise (MacManus *et al.*, 2013). The use of the internet and online resources without threat awareness can have disastrous results for organizations and individuals alike.

When unaware and untrained government employee accesses the internet while at work, they can put an immense amount of constituent and transactional data at risk. Government employees are often pressured to meet deadlines and the subsequent sense of urgency often lures them into a secure state of mind. This lack of situational awareness regarding their security habits has “shown that the human firewall in cybersecurity is often compromised, with potentially catastrophic consequences for users, the organizations they represent, and their



clients” (Chowdhury *et al.*, 2019, p. 1291). It is also important to note that for many “meeting cybersecurity requirements often holds users back in their primary work tasks” and therefore “perception of the importance of cybersecurity in the organization further deteriorates” (p. 1298). Chowdhury *et al.* (2019) further state that with regard to security policies, security procedures, and technical controls “the likelihood of success of these countermeasures ultimately depends on the actual behaviour of security practitioners” as these controls can seem to overcomplicate and burden employee operations (p. 1293). Costa *et al.* (2019) further suggest that these security controls as established by organizational administration help disseminate how employee “behaviour plays a fundamental role in the security of the information, of the equipment, and of the systems, both in their workplace and home (p. 2036). Kortjan and Solms (2014) further state that management can further an organization’s cybersecurity goal by being supportive of security initiatives, “that promoting cyber-security awareness would contribute greatly towards cyber-security as a whole” (p. 29).

Following a proper cybersecurity regimen complemented by adequate training and exercises allows employees “to focus on continually improving citizen experience without having to worry about the disruption” of services and “organizational processes, or perhaps worse, that their needs may go unmet” (Axelrod, 2019, p. 1). Especially in an environment where data security is key to serving the public’s interest and maintaining trust, all of which can be enforced by proper training and security habits.

However, for training to be successful, the appropriate content and approaches should be considered, and security awareness content developers should as Adorjan and Ricciardelli (2019) recommend, by developing content that gives the learner the “ability to relate to and apply such messages in their day-to-day experiences,” while trying to avoid putting excessive “focus on

dangers that are both highly unlikely and at odds with” the learner’s professional and social experiences (p. 432). Daengsi *et al.* (2021) argue that “the risks from this kind of threats can be reduced if the employees have cybersecurity awareness” (p. 102). This sentiment is echoed by Costa *et al.*, 2019; Heartfield and Loukas, 2018; and Kortjan and Solms, who agree that awareness training is key to employees being able to identify suspicious activity and reporting it to their security team. Diaz *et al.*, (2020) and Daengsi *et al.*, (2021) further recommend that training should also be complemented with simulations, which can facilitate greater participation and learning while identifying deficiencies in training and training content. Peker *et al.*, (2016) stated, “An adequately interactive security awareness module that demonstrates the shocking consequences of careless cyber habits of common Internet/technology users will effectively increase awareness at a large scale” (p. 4). Organizations that invest in cybersecurity training for their employees make them “part of the solution instead of part of the potential problem” (Costa *et al.*, 2019, p. 2036).

Some organizations may still be somewhat apprehensive about the provision of training for their employees, including but not limited to cybersecurity awareness training. Researchers agree that there are many benefits to organizations investing in cybersecurity awareness training and that empowering its employees has the added benefit of improving the organization’s overall security posture and cyberattack resilience (Costa *et al.*, 2019; Diaz *et al.*, 2020; Peker *et al.*, 2016, and Daengsi *et al.*, 2021). For an organization to understand the added benefits of implementing a cybersecurity awareness program, Tirumala *et al.* (2019) suggest that “the importance of cybersecurity awareness is established by presenting various statistics, followed by the current implementations for cybersecurity awareness,” this establishes the organization's current baseline (p. 1). Also, Oancea *et al.* (2019) further state that “most cyber-attacks exploit

the vulnerability of users and only some of them exploit the technical flaw” and the only remedy to that vulnerability is to improve the security-based situational awareness of their workforce (p. 46). The validity and efficiency of the training can then be assessed via a survey as in the case of this study and as Tirumala *et al.* (2019) suggest a “survey provides a comprehensive understanding of cybersecurity awareness” of an organization post-training (p. 1). Yazdanpanahi (2021) argues that “when employees are well educated and trained, they can also be valuable and the first line of protection against cyber threats,” however organizations “must have consistent training classes and anti-phishing campaigns throughout the year to keep employees aware” of the ever-changing threat landscape (p. 3). Cybersecurity training courses became mandated when the State of Texas passed House Bill 3834 in 2019 and House Bill 1118 in 2021, for all state and local government employees as a result of the increase in cyberattacks across the nation and Texas specifically (Yazdanpanahi, 2021).

This lack of cyber awareness is leading to compromises of business data, corporate networks, and personal identity information for groups and individuals alike (Daengsi *et al.*, 2021; Kortjan and Solms, 2014; Olmstead and Smith, 2017). While many organizations do not know how to properly disseminate information and training on cyber awareness, most individuals do not know they should be aware of cybersecurity concepts while on the internet (Peker *et al.*, 2016; Olmstead and Smith, 2017). The application of traditional corporate training courses often takes much of a worker's time and productivity away and is mostly seen as a chore, usually not taken seriously. This literature review is offered to provide a synopsis of the relevant cybersecurity literature and further, the understanding of the effectiveness of cybersecurity training to increase cybersecurity awareness in a population.

There is a consensus between the national news and the research that there is a vital need for cyber awareness training to improve the cybersecurity of both organizations and individuals (Diaz *et al.*, 2020; Costa *et al.*, 2019; Vishwanath, 2021; Skertic, 2021). Kemper (2019) states that “in 2019, employees still aren’t convinced about their company’s vulnerability to cybercrimes, even though 34% of people experienced a breach of their personal data in 2017.” He further states that for organizations, “employees pose the greatest cybersecurity threats” to their corporate data and networks, especially when they are not trained to be cybersecurity aware (Kemper, 2019, p. 11). This is further exacerbated by a culture of internet users that share passwords and consistently click on links in e-mails or websites that are unsafe. They simply do not understand or are aware of the repercussions of their actions and their role in safeguarding their company’s data assets or even their data. One way to change this culture and in agreement with most security experts is through education if an employee touches a computer, they need cybersecurity training to make them cybersecurity aware and responsible for their actions online (Costa *et al.*, 2019; Heartfield and Loukas, 2018; Kortjan and Solms, 2014; CISA, 2020).

### **Conceptual Framework**

A considerable number of information security compromises are the result of human error, negligence, or perhaps even a lack of awareness regarding cybersecurity concepts (Diaz *et al.*, 2020; Chowdhury *et al.*, 2019; Tirumala *et al.*, 2019). While training can work as a mitigation tool, other factors can both impede or improve an employee’s functional awareness and behavior in response to cybersecurity incidents. Sherif *et al.* (2015) argued that the development of a security culture within the organization was another method for improving behavior that would lead to fewer cybersecurity incidents and developing a framework for establishing that security culture. Sherif’s conceptual framework presents how information

security culture may serve as a model for improved behavior and awareness from the organizational level up to the national level.

Figure 4 below depicts an adaptation of Sherif's (2015) conceptual framework. The adaptations include adding variables and factors that influence cybersecurity culture within an organization. The framework consists of components including management's influence, the employee's awareness, their acceptance of cybersecurity concepts, and the anticipated changes to behavior. The values are gathered into the four steps required to create cyberculture and improve security compliance within the framework proposed by Sherif *et al.* (2015). The framework adapted for this study consists of using Sherif *et al.*'s (2015) parent variables for security compliance within organizations but adds steps as sub-variables that have been identified according to the role, they play in influencing the employees' intention to comply with security policies and action regarding cybersecurity incursions.

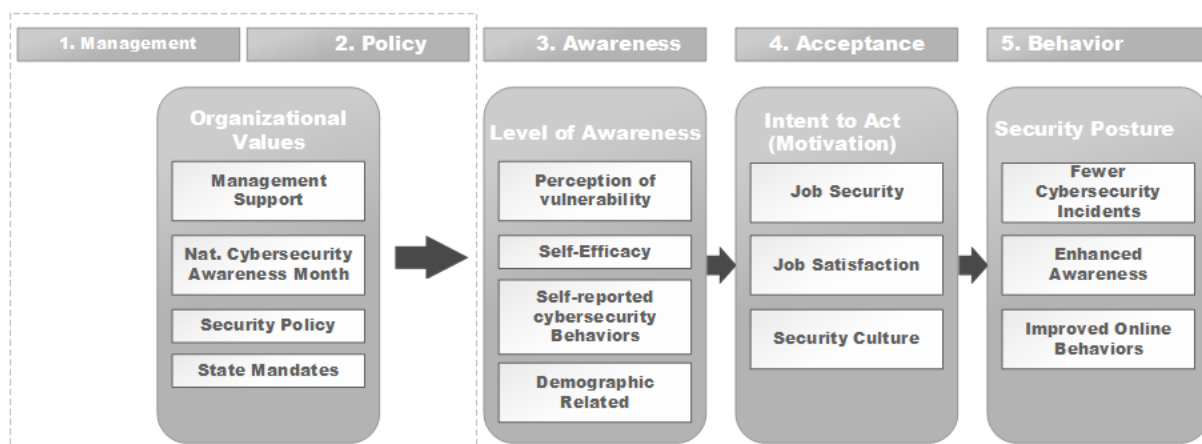


Figure 4: Study framework adapted from Sherif *et al.* (2015)'s conceptual framework for information security culture.

The framework in Figure 4 above presents the organizational steps required for an improved security posture, enhanced awareness, and the required knowledge of information

security provided by cybersecurity awareness training, and management support. Employees are therefore equipped to do their job in a way that is consistent with acceptable information security practices that keep their organization secure while improving job security and organizational security posture.

Sherif *et al.* (2015) argued that an organization's security culture begins with the support of management and is included within "the fields of corporate governance, information security, and organizational culture" (p. 438). Corporate values help establish the "beliefs, assumptions and values shared" of the organization's employees (p. 438). Those values are often driven by corporate policies, including but not limited to those referring to cybersecurity and acceptable use of Internet communications technologies (ICT). These values are often adopted with less resistance when employees can see management's active role in the promotion of specific events including but not limited to National Cybersecurity Awareness Month (NCSAM) in October. Alternatively, Sherif *et al.* (2015) further suggest that "some aspects of an organization's security culture have evolved as a logical response to security threats, and are espoused by the management of the organization" (p. 439). In many cases, the need for security adoption is the result of a compromise, resulting from a lack of awareness and preparation. Lastly, a policy can be driven and sometimes enforced by state and federal mandates as in the case of Texas House Bill 3834, which requires government employees in Texas to take an annual cybersecurity course. Chowdhury *et al.* (2019) suggest that when organizations disseminate cybersecurity courses, it drives awareness within the organization and can help expose issues of self-efficacy with technology and a user's perception of vulnerability when working with ICT. Kortjan and Solms (2014) further argue that "education plays a critical part" in an organization's efforts "in cultivating a culture of secure behavior" (p. 29). Determining the level of cybersecurity

awareness within an organization can allow security groups within the organization, often the IT Department, to work towards improving awareness and identifying if there is a lack of awareness within specific demographic groups, allowing them to effectively target those groups to receive additional reinforcement. Situational awareness is the eventual behavioral change that leads to the acceptance of the need to be more cautious of online behaviors and the usage of internet-connected technologies (Heartfield and Loukas, 2018; Catota, Morgan, & Sicker, 2019).

As a result of the need for awareness of cybersecurity concepts, the acceptance of cybersecurity policies, and the expected behavioral change, the framework developed by Sherif *et al.* (2015) was adapted for this study and includes motivators (intent to act) for cybersecurity acceptance and the improvement to an organization's security posture as a result of better employee behavior with regards to the use of internet-connected technologies. The idea of intention and the resultant action was discussed by Baier (1970), who suggested that a person cannot do what they do not know how to do, they can only learn to do something. An employee may be motivated to act responsibly online through the application of training and can therefore act by following the techniques and concepts learned through the provided cybersecurity training. Motivation can also be related to subjective norms and attitudes within the organization, issues related to job satisfaction, and even job security as a result of failing to act accordingly to prevent a cybersecurity incident. This type of motivation would be related to models such as the Theory of Reasoned Action as proposed by Salgues (2016), where the employee's action is the result of a causal chain of beliefs and attitudes, developed by cybersecurity training, management support, and their acceptance of how cybersecurity concepts impact their organization and ultimately their job satisfaction and improve their job security. This ultimately creates the cybersecurity culture recommended by Sherif *et al.* (2015).

Sherif *et al.* (2015) suggest that a positive and active cybersecurity culture based on their framework, or the used modified framework can lead to an organization with employees that have enhanced cybersecurity awareness that makes them less of a target for cybercriminals and even less of a threat to the organization's security posture. Organizations including but not limited to the Cybersecurity and Infrastructure Security Agency (CISA) and the Department of Homeland Security (DHS) have developed programs to improve the online behavior of the average person, working towards behaviors that remind them to think before they click (Kessler and Ramsay, 2013; CISA, 2020). An organization with a functional cybersecurity culture theoretically has a good security posture and has a lowered risk of cybersecurity compromise (Costa *et al.*, 2019; Peker *et al.*, 2016). Yazdanpanahi (2021) further state “a strong security culture that can go a long way toward minimizing threats for city government” (p. 4).

### **Factors Influencing Cybersecurity Awareness**

Cybersecurity awareness for government agencies is critical as they are required to safeguard large amounts of constituent data under their care (Schürmann *et al.*, 2020; Macmanus *et al.*, 2013; de Bruijn and Janssen, 2017). Furthermore, government employees are historically targets for phishing attacks by cybercriminals, especially when time pressure and deadlines can make them less cautious and more susceptible (Schürmann *et al.*, 2020; Chowdhury *et al.*, 2019; McCormac *et al.*, 2017; Kemper, 2019). A lack of awareness of cybersecurity concepts can lead to the vast amounts of constituent data collected by government agencies being at risk of being compromised. Government employees require the specific skills and competencies needed to contend with and mitigate cyber-related risk (Yazdanpanahi, 2021; Anwar *et al.*, 2017). There are several factors thought to influence cybersecurity awareness. This section will address the



four most common (1) Cybersecurity education, (2) Measuring Awareness, (3) Demographic factors, and (4) Threat perception and mitigation.

### **Cybersecurity education**

The educational process can be used to instill a cybersecurity-aware mindset. The use of educational strategies can be used to “apply new ways of thinking, new understanding, and new strategies to our nation’s response to cyberattacks” (Kessler and Ramsay, 2013, p. 36).

Employees' understanding of cybersecurity concepts allows the average internet user to identify and possibly mitigate cyber threats, thereby improving self-efficacy (Olmstead and Smith, 2017b). Kessler and Ramsay (2013) further stated that “education provides individuals with a systemic understanding” of the discipline that is cybersecurity (p. 40). Management support of cybersecurity education can improve awareness and along with policy, procedures, and technology allows organizations to improve their security posture.

### **Paradigms for Cybersecurity Education**

The U.S. Homeland Security Agency has been one of the government agencies leading the charge for more cybersecurity education (Kessler and Ramsay, 2013). Kessler & Ramsay (2013) state that the federal government has tasked academic institutions with taking “an active role in Homeland Security education” with the passing of The Homeland Security Act in 2002 (p. 37). Government research has shown that the United States has “a shortage of cybersecurity expertise” and little effort was being made to improve our chances of surviving the next “Cyber–Pearl Harbor” (Kessler & Ramsay, 2013, p. 36). A lack of cybersecurity awareness among its denizens coupled with an aging, yet critical infrastructure does give rise to the concerns that the U.S. Department of Homeland Security (DHS) has placed cybersecurity on the nation’s shortlist of security concerns. Kessler and Ramsay (2013) propose paradigms for the development of

cybersecurity programs and their integration into academic curricula. Furthermore, the authors suggest that attempting to force students into cybersecurity programs will not work and that learners do not need full expertise in the subject matter to understand the threat posed by a lack of cybersecurity.

Kessler and Ramsay's (2013) paradigm addresses teaching Homeland Security learners the operational and applicable side of cybersecurity concepts, which the authors assert is lacking from traditional cybersecurity training.

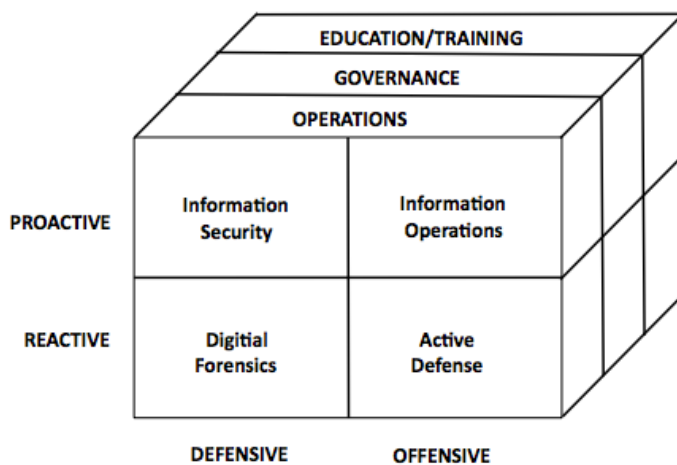


Figure 5: Paradigms in information assurance/cybersecurity

The proposed curriculum is inclusive of daily operations, structured management, policy, procedures, roles, and applicable laws. This will train learners on the specific skills and competencies needed to contend with cyber-related risk, “whereas education provides individuals with a systemic understanding” of the discipline that is cybersecurity (Kessler & Ramsay, 2013, p. 40). The suggested curriculum and pedagogy are general and not overly technical where learners may become discouraged. The proposed paradigm also recommends

the use of techniques including scaffolding to allow learners to apply their knowledge to other aspects involving the nation's security.

When applying a paradigm such as this to consumer-based training, applying a similar pedagogy that allows for systemic understanding, is not overly technical, and most importantly applicable to the learner's daily routine is important (Yazdanpanahi, 2021; Carlton, 2016).

Cybersecurity should be consistent and relevant to the learner's role within the organization.

The considered curriculum is suggested by The Department of Homeland Security as a means to help mitigate the threat posed by cybercriminals to their organizations. Homeland Security has raised concerns about the nation's cybersecurity, and state and local agencies are a primary target (Kessler and Ramsay, 2013; Macmanus *et al.*, 2013; Schürmann *et al.*, 2020). They explain that a vested interest in their own agency's security is key, as they are likely as much a target as the national government. Education is a valuable tool that can improve local government agencies' chances of surviving a cybersecurity attack and lowering their overall cyber risk (Yazdanpanahi, 2021).

### **Education Is Critical To Cybersecurity Awareness**

Kortjan and Solms (2014) state that "although cyberspace offers an endless list of services and opportunities, it is also accompanied by many risks, of which many Internet users are not aware" (p. 29). Kessler and Ramsay (2013) argue that it is difficult "to provide technical literacy for a student population that is, in general, not overly technically inclined," making it harder to educate employees and individuals on what may be considered highly technical content that they didn't know they needed (p. 41). A single employee that is not cybersecurity aware can cost organizations millions if not billions of dollars in damages in addition to the costly embarrassment of having a data breach (Skertic, 2021; Kostyuk and Wayne, 2020). These

breaches or cyber ransoms can often mean catastrophic losses for organizations, which translate to significant revenues for cybercriminals. Kortjan and Solms (2014) recommend that the “target audience should be presented with topics that are relevant to them,” thus, making the content more approachable and user-friendly can theoretically lead to more cyber security-aware learners, thus reducing the odds of having a cybersecurity incident (p. 33). This was furthered by Schürmann *et al.* (2020) who suggested that “cybersecurity training must be perceived as relevant by the target group for it to be effective” (p. 199).

Kortjan and Solms (2014) further found that “education plays a critical part” in an organization's efforts “in cultivating a culture of secure behavior” (p. 29). People and workers depend on the Internet for the majority of day-to-day activities. Diaz *et al.* (2020) state that even in a digital society, the lack of cybersecurity awareness among active internet users can their personal information at risk, that the increased use of “social engineering to exploit users into giving up valuable and confidential information” is rapidly increasing (p. 53).

This is furthered by Tirumala *et al.* (2019) who state that cybersecurity is “misunderstood by many people, cybersecurity is not confined to securing computers on the internet,” it involves the human factor as much as the machine (p. 1). The uninitiated internet user is surprisingly susceptible to the tactics associated with cybercrime, which “at present, social engineering is one of the widely used approaches for stealing individual information and private data” (p. 2). The application of educational content could result in a behavioral change when it comes to the mitigation of cybersecurity attempts, through an employee’s knowledge and understanding of cybersecurity concepts (Kostyuk and Wayne, 2020; Peker *et al.*, 2016). The world is gradually becoming more interconnected, everyone shares the responsibility of securing cyberspace (Kessler and Ramsay, 2013).

## **Improving Employees' Capacity For Cybersecurity Through Malware Training**

He *et al.* (2020) investigated methods to improve the effectiveness of cybersecurity training media by observing the use of multimedia along with the inclusion of printed cybersecurity risk reports. Also, they administered pretest-posttest surveys along with a training program that consisted of different combinations of media. Their study observed the use of multimedia along with the inclusion of printed cybersecurity risk reports. Their study consisted of a pretest-posttest survey along with a training program that consisted of different combinations of media. The objective was to see if the different combinations of media changed the effectiveness of the training and to determine if “any changes of their perceptions of vulnerability, severity, self-efficacy, security intention as well as their self-reported cybersecurity behaviors” (p. 208). Their study resulted in that while multimedia makes little difference, the act of providing training or “people patching” helps learners to recognize, mitigate, or simply avoid cybersecurity threats (p. 209). This includes consistently updating employees about new cyber threats and how to identify them, in order to avoid workplace disruption. Another important consideration when providing training and raising its effectiveness is to “relate cyber awareness to employees’ personal life, family, and home, in order to be more engaging and to encourage employees to change their cybersecurity behavior both personally and professionally (p. 210). Essentially any effort on the part of an organization to put their employees in front of cybersecurity awareness training can be beneficial, the higher the quality of the training, the better the results (Daengsi *et al.*, 2021; Yazdanpanahi, 2021; Peker *et al.*, 2016; Costa *et al.*, 2019; Yazdanpanahi, 2021).

## Effectiveness of Training on Cybersecurity Incidents

Heartfield and Loukas (2018) and Carlton (2016) suggest that self-efficacy is one of the largest concerns with the deploying or administering of cybersecurity training. Kweon *et al.* (2019) used the number of cybersecurity incidents and their relation to cybersecurity training to measure the effectiveness of a proposed training. The researchers found that there was a positive correlation between decreased or slowed incidences of cybersecurity threats and employees' participation in cybersecurity training. Correspondingly, if the incidences of cybersecurity threats increased or remained the same after training, the researchers could state little to no correlation between the incidences of threats and employees' participation in cybersecurity training. Furthermore, the authors reiterate the concerns that their data, although intangible, is part of their core assets and, therefore, critical for most organizations. The damages arising from cybersecurity incidents are not intangible, but physical and have a monetary cost associated with them (Kweon *et al.*, 2019). Moreover, the authors agree that cybersecurity training and education enhance an employee's ability to mitigate cyber risk. Training an organization's employees generally have a positive effect, in that it helps to protect an organization from external threats.

Kweon *et al.* (2019) further the discussion that human error is one of the major concerns and often the cause of a cybersecurity incident. Many organizations are willing to invest in physical security but fail to see the return on investment (ROI) in the application of cybersecurity training (Kweon *et al.*, 2019). Recent research has shown that ransomware-related cyberattacks are on the rise and targeting employees with tactics including social engineering and phishing, attacks which often come at a higher cost (Kweon *et al.*, 2019; Yazdanpanahi, 2021; Kostyuk and Wayne, 2020). Kweon *et al.* (2019) also posit that understanding the level of awareness in

an organization is critical to mitigating cyber risk. Their study examined the actual impact of cybersecurity training by observing and quantifying the number of security incidents post-training. Kweon *et al.* (2019) also recommended that cybersecurity training also include managers and department heads, as their survey placed 28% of the blame for security breaches on management's lack of awareness and "prioritizing of cybersecurity" (p. 4). Furthermore, they argue that organizations where management has a passive stance on cybersecurity, also have employees who neglect their cyber responsibilities. Moreover, the authors observed that there is a shortage of qualified technical staff, even more, so those with training skills. In the end, the result of the Kweon *et al.* (2019) study suggested that more time with cybersecurity concepts and training would be more beneficial in reducing cyber risk. This is consistent with the recommendation that cybersecurity training not only needs to be relevant but also consistently provided (Kortjan and Solms, 2014; de Bruijn and Janssen, 2017; Adorjan and Ricciardelli, 2019; Yazdanpanahi, 2021).

### **Measuring Awareness**

Understanding the level of cybersecurity awareness in an organization can be the difference between surviving or succumbing to a cyber-attack, that awareness is measured within that organization's workforce. An organization's employees are often considered the weakest link in the organization's security posture and are consistently the cause of a compromise, this is a well-known issue among many cybersecurity professionals (Diaz *et al.*, 2020; Chowdhury *et al.*, 2019). Whether using surveys or phishing exercises, measuring an organization's cybersecurity awareness allows management to understand what their workforce knows and if additional training or education is needed to improve their cybersecurity awareness. Researchers have categorized levels of cybersecurity awareness as low, medium, and high and even used data

analytics; to establish how neglectful or attentive internet users are toward the proper usage of technology and knowledge of cybersecurity concepts (Zwilling *et al.*, 2020; Tirumala *et al.*, 2019). Assessing the effectiveness of the training program and whether it can improve the awareness of cybersecurity concepts in a population helps to improve learning content for cyber risk awareness and supports organizations attain a better cybersecurity posture.

Cybersecurity knowledge and awareness can be maintained by including the regular delivery of both awareness and educational content post-study. These include but are not limited to periodic assessments in the form of “fake phishing” e-mails that were presented to random employees to gauge if the population of learners was benefiting from the adopted learning materials or if further instruction or training was required. The dissemination of training programs by organizations must “consider the implications of end-user-driven risks, they should also consider the opportunities to mitigate these risks and create a workforce that has the knowledge to make knowledgeable choices” (Miller, 2017, p. 13) and can be part of the solution rather than part of the problem. A workforce that is cybersecurity aware improves an organization's security posture and is therefore at a lower risk of cyber-related incidents including but not limited to cybercrime.

### **Factors Related to Cybersecurity Awareness**

Daengsi *et al.* (2021) argue that the threats associated with cybersecurity compromise can be reduced if employees have cybersecurity awareness. Kortjan and Solms (2014) further that this awareness can be improved by providing employees with relevant information and training in cybersecurity concepts. Daengsi *et al.* (2021) suggest that the dissemination of cybersecurity “best practices, concepts, policies, assurance, guidelines, safeguards, actions, risk management methods, training, tools and technologies that can be used to protect users' assets and the



organization environment” (p. 102). Daengsi *et al.* (2021) tested cybersecurity through the use of attack simulations (phishing) in a comparison between company departments and “found that there are significant differences in cybersecurity awareness level between Thai employees from technology-based departments (e.g., IT department) and social-based departments (e.g., HR department) within the same organization” (p. 102). They further found that cybersecurity awareness improved after they were involved with the cybersecurity awareness development processes. Furthermore, Daengsi *et al.* (2021) and Diaz *et al.* (2020) argued that cybersecurity awareness is impacted by several demographic factors, including educational background, work experience, field of study, gender, age, and socioeconomic status. Moreover, they defined cybersecurity awareness as the response to cyber threats and cyber-attacks properly, through both technical and the efforts of their workforce. Yazdanpanahi (2021) and Costa *et al.* (2019) suggest that the return on investment for the provision of cybersecurity awareness training is their workforce’s ability to protect their company’s assets against cyber threats, thereby making them “part of the solution instead of part of the potential problem” (p. 2036).

### **Cybersecurity Awareness and Knowledge**

The growth of information technology and the internet has brought about a new consumable resource as well as a new type of consumer, the “netizen” or digital citizen (Zwilling, 2020, p. 1). However, these new consumers do not often have sufficient awareness or even the minimum required knowledge to protect themselves from cybercrime while online. This unsafe behavior leads to them becoming the weakest link in the security posture of the organizations that employ them. A study by Zwilling *et al.* (2020) categorized levels of cybersecurity awareness as low, medium, and high; which established how neglectful or attentive an internet user is toward the proper usage of technology and knowledge of cyber threats. They

also defined cybersecurity awareness as “the degree of understanding of users about the importance of information security and their responsibilities and act to exercise sufficient levels of information security control to protect the organization’s data and networks” (Zwilling, 2020, p. 2). Therefore, the need for additional training is required to help mitigate the lack of cybersecurity awareness among individuals and organizations as a whole. These training courses have become mandated in some organizations, including but not limited to government entities as a result of the threat of cybercrime.

The dependency on internet-based technologies has grown across all modern organizations both public and private, and knowledge of cybersecurity threats has not grown at the same pace among internet users. Research even found that “self-identified experts had less cyber hygiene knowledge than self-identified non-experts,” meaning that the rapidly changing landscape of cybersecurity requires constant and consistent training (Zwilling, 2020, p. 3). Behavior changes are one of the ultimate goals of cybersecurity awareness. An employee’s behavior related to risk-taking and self-efficacy are good indicators of their threat level to the organization. This also establishes the need for additional awareness training as a means to enact sustainable behavioral change, while increasing the employee’s knowledge of cybersecurity.

### **Surveying internet usage and cybersecurity awareness**

Both public and private business sectors are moving more and more of their services at an accelerated rate to the internet, called cyberization. As a result of this rapid growth of internet usage, most of which has taken place in the last decade, cybercrime or unlawful acts committed on the internet or cyberspace have also increased. These cybercrimes are requiring for institutions to provide institutions provide some form of adequate cybersecurity awareness training as a deterrent to cybercriminals as “employees pose the greatest cybersecurity threats to

businesses” (Kemper, 2019, p. 11). This is further argued by Peker (2016) when stating that “the need for creating a culture of safe cyber behavior is growing significantly” (p. 3). The only way to establish this cyber-aware culture is through proper instructional courses and well-established and disseminated security policies.

To develop a cyber awareness course, the current level of awareness needs to be measured within the targeted population. Tirumala, Valluri, and Babu (2019) suggest that metrics could be collected to measure existing knowledge, using a “survey [that] provides a comprehensive understanding of the cybersecurity awareness” of a given population (p. 1). Interestingly, Tirumala *et al.* (2019) survey did provide some valuable metrics including that “over 80% connects to the internet through a home broadband connection,” that “only 38% of total participants” have implemented some form of active internet security protection, and that “that about 10% are little or not at all concerned about security,” which further bolsters the need for cyber awareness (p. 2). These concerning metrics, in turn, can be used to guide instructional designers in the development of training content based on Tirumala *et al.* (2019) who proposed a “framework that leads to the process of implementing cybersecurity awareness” (p. 1). A framework that takes passwords, cyber-bullying, and common cybercrime techniques into account. Assessing the mindset and existing knowledge of a population helps to prepare learning content for cyber risk awareness.

### **Improving cybersecurity awareness with data analytics**

While the statistical analysis data by Tirumala *et al.* (2019) provides data for the development of a cyber awareness framework to be used in the development of course materials, it does not consider the qualitative “human-factor” data regarding the value of the course content to the individual. If instructional material, regardless of the topic, does not appeal to the learner

or is formatted in such a way that they can understand it, it can be deemed ineffective. Korpela (2015) states that a consequence of an ineffective cyber awareness program is that it usually ends with a compromise of security and the loss of “executives’ sponsorship and cybersecurity professionals’ respect” (p. 72).

Korpela (2015) recommends using data analytics to properly assess the risk to an organization given that “if end users are not aware of the security risks inherent in their actions” they can be a serious flaw in their organization's security posture (p. 75). She stated that for a cybersecurity awareness program to be successful organizations need to identify users that are at risk due to a lack of cybersecurity awareness and understand how that awareness is best achieved by learners. These two data points can help improve the overall metrics collected. She also argues that “organizations should not assume only the technologically illiterates would fall” for the devices of cybercriminals (p. 73). She states that even users “with no access to confidential information” can be a threat to an organization’s security posture, due to handling tasks for higher-ranking officials within the organization (p. 73). While statistical data is useful, data analytics should be used to conduct a “human risk assessment to understand the risk level associated with each end-user and therefore deploying a risk-based cybersecurity awareness and training program” (p. 75). Utilizing the risk assessment allows educators to use a constructivist methodology to build scaffolding material to build upon existing cyber awareness deficiencies.

### **Raising cybersecurity awareness**

Peker *et al.* (2016) state that cybersecurity and the need for cyber awareness are a direct result of society's increasing “reliance on digital equipment and programs to manage our daily lives, including the transmission and storage of personal information” (p. 1). The authors explain that “a common ignorance of people in managing and protecting their information in

cyberspace” (p. 2), is why cyber awareness training is needed by organizations and individuals alike. They exemplified their statement by presenting a common phishing attack story and how easily a user was duped into sharing personal information and further stated that “as a result of this ignorance, threats of cybercrime are continuously rising” (p. 2). This includes data breaches for large organizations and governmental institutions, mostly due to reckless uninformed human behavior. Simply stated, the authors observed that the “digital world provides many conveniences but also poses new risks that often go unknown or unnoticed” because “society did not plan, create, and disseminate education about cyberspace quickly enough to match the increased use of cyberspace” (p. 2).

In general, people do not know they are not being careful until a compromise happens, or they are educated about proper internet usage etiquette. These data breaches and personal compromises are exemplary justifications for “the need for creating a culture of safe cyber behavior” (p. 3). In the case of Peker *et al.* (2016) study, they focus on college students and used interactive learning modules, not unlike those found in a microlearning lesson to “improve college students’ awareness of cybersecurity” (p. 4). Programs such as this are being developed by organizations in all sectors of business, including but not limited to public, private, and educational in order “to increase awareness and responsiveness to cybersecurity threats” (Peker *et al.*, 2016, p. 5).

### **Cybersecurity Awareness in Government**

Schürmann *et al.* (2020) discussed that government employees, especially those who conduct elections, should take a cybersecurity awareness course due to the amount of constituent data they oversee and that historically they are often spear-phishing targets. However, Schürmann *et al.* realize that “cybersecurity awareness training has a bad reputation for being

ineffective and boring” (p. 196) and that some modifications to the development and assessment are required to make them more effective for short-term retention of cybersecurity concepts and that this training helps to protect an organization from security breaches and prepares employees to help defend against cyber-attacks. They suggest that cybersecurity training sharpens “a user’s common sense and the ability to recognize, react, and mitigate an imminent attack, and to install a designed behavior in connection with security” (p. 196). Therefore, Schürmann *et al.* suggest that training needs to be “methodologically relevant and consistent” after a security analysis is conducted to understand the organization's security risk factors, which helps to establish relevancy and help to change employee behavior.

Schürmann *et al.* used Kirkpatrick’s Model to evaluate the effectiveness of cybersecurity training by using a pre-and post-training survey to understand “how intellectual capability has changed from before the training” (Schürmann *et al.*, 2020, p. 203). Their study was one of the first to look at e-learning for short-term retention of cybersecurity concepts.

Schürmann *et al.* (2020) define security awareness as having three levels, perception, comprehension, and projection. This suggests that the cyber security-aware employee effectively is more “aware of that there are potential,” able to “understand and assess the dangers of security risks,” and “able to anticipate future situations” involving cybersecurity risks (p. 197). Therefore, improving an employee’s status as the weakest component within their organization’s security framework and improving their organization's security posture. The human factor or more colorfully “the human firewall” is consistently breached and is a well-known issue among many cybersecurity professionals (Diaz *et al.*, 2020; Chowdhury *et al.*, 2019). Furthermore, Catota *et al.* (2019) state the importance of increasing learner engagement with “cybersecurity

awareness and education can be essential against a subset of attacks,” while improving the learners' personal protective measures (p. 16).

### **Using Phishing to Test Awareness**

User susceptibility and behavior are critical factors to understand within any organization that hopes to mitigate cyber risk. While risk assessment helps to determine an organization's, risk factors and points of susceptibility, cybersecurity awareness training aims to change employee behaviors. Diaz *et al.* (2020) studied these factors within an academic environment, looking for a correlation between awareness and being susceptible to a mock-phishing exercise. The authors conducted that regardless of industry or business sector, “the human factor or error is responsible for 95% of security incidents” (p. 53), which is a consensus shared by other researchers. Their study consisted of fake phishing attempts against the studied population at the University of Maryland, the population was initially unaware of the study. The phishing of fake email attempts looked authentic enough that only the trained eye could spot the not-so-obvious red flags that would delegitimize the email. The phishing attempt was significant enough that the campus technology department (IT) alerted the campus of a campus-wide phishing attempt. The authors' concern about susceptibility was answered when “of the 1350 students randomly selected for this study, 1246 (92%) opened” one of the three phishing e-mails (p. 59). The study found that the more educated or advanced a student was the less likely they were to click or be susceptible to phishing attempts. However, contrary to the researchers' expectations some of the more technical students did fall victim to the phishing attempt as a result of what was likely an overestimation of their knowledge of phishing.

Chowdhury *et al.* (2019) state that in most organizations, the human factor involved will always be the weakest link and most exploitable point of any cybersecurity risk scenario.

Subsequently, the consideration of the human factor in information security has become increasingly important for organizations, especially government agencies (McCormac *et al.*, 2017). Diaz *et al.*'s (2020) study found that even the most technical employee can lack the awareness needed to mitigate cyber risk. Even the more tech-savvy can overestimate their knowledge of cybersecurity concepts and be susceptible to more sophisticated attacks. This was confirmed when “nearly 70% of the tech-savvy students clicked the phishing link” (p. 65) that would initiate a compromise. Furthermore, Costa *et al.* (2019) recommend that all organizational employees participate in an organization-sponsored cybersecurity awareness training, to “enable the users to understand that their behaviour plays a fundamental role in the security of the information” (p. 2036).

### **Demographic Factors Impacting Cybersecurity**

The literature is consistent in that many cybersecurity breaches are the result of human error, a lack of cybersecurity awareness, and even considering employees as the weakest link in the organization's security posture (Fatokun *et al.*, 2019; Diaz *et al.*, 2020; Miller, 2017; He *et al.*, 2020; Kweon *et al.*, 2019; Heartfield and Loukas, 2018). Demographics can play a large factor in how an organization's employees receive and apply cybersecurity concepts (Olmstead and Smith, 2017; Fatokun *et al.*, 2019; Adorjan and Ricciardelli, 2019; Daengsi *et al.*, 2021). Fatokun *et al.* (2019) further argue that these demographic factors can be used to enhance effectiveness and perhaps even better target cybersecurity awareness curriculum. The idea that demographic factors such as age, gender, and level of education affect a learner's ability to comprehend the threats associated with cybersecurity compromise is not a new one, as several authors have found that these factors have subtle but important effects on cybersecurity (Anwar *et al.*, 2017; Fatokun *et al.*, 2019; Tirumala *et al.*, 2016).



Age has been one of the more studied demographic factors, especially with the belief that many so-called “digital natives” are expected to perform better with technical content as a result of “having been exposed to technology from a young age” compared to older generations with less exposure (Haney and Lutters, 2017, p. 6). When studying gender, differences have been found in the perceptions of males versus females regarding self-efficacy and perceived risk of cybersecurity threats. In a study, Fatokun *et al.* (2019) found that males scored better than females regarding technical concepts. Education is another factor associated with the belief that individuals enrolled in higher levels of education are more exposed to current information, including but not limited to cybersecurity awareness (Carlton, 2016; Kostyuk and Wayne, 2020; Olmstead and Smith, 2017). Fatokun *et al.* (2019), conducted a study where younger undergraduate students fared better than older post-graduate students. Several studies have shown that the age of the learner may play a larger factor in education (Fatokun *et al.*, 2019; Diaz *et al.*, 2019; Tirumala *et al.*, 2019).

### **Gender Differences in Cybersecurity Behaviors**

Anwar *et al.* (2017) continue the argument that the human factor is a critical weakness in any organization’s security framework and that there is a need “to develop effective cybersecurity training programs for employees in the workplace, it is necessary to understand the security behavior of both men and women” (p. 437) because of their different perspectives on cybersecurity concepts. The researchers used a Likert-based survey to determine their cybersecurity beliefs and behaviors. The study found that females were more “concerned about privacy” and “are more likely to comply with security policy than men” (p. 440). It also found that males “place a greater influence on attitude toward using technology than women” (p. 440). More importantly, Anwar *et al.* (2017) determined that the ability to perceive and accept risk

varies by gender, females are generally more concerned with perceived risk as opposed to their male counterparts.

Anwar *et al.* (2017) state that the differences based on gender “are statistically significant gender-wise differences in terms of computer skills, prior experience, cues-to-action, security self-efficacy, and self-reported cybersecurity behavior” (p. 440). Research shows that gender plays a role in cybersecurity awareness, especially concerning self-efficacy with technology (Tirumala *et al.*, 2016; Diaz *et al.*, 2020; Fatokun *et al.*, 2019). Anwar *et al.* (2017) further argue that as a result of these differences, curriculum developers may consider these differences during the development of cybersecurity awareness courses. Researchers agree that addressing these gender-related differences in behavior, perceived threat, perceived risk, and genuine attitudes toward cybersecurity concepts can make the difference between an organization facing a compromise of their cybersecurity or remaining cyber secure (Tirumala *et al.*, 2016; Diaz *et al.*, 2020; Fatokun *et al.*, 2019; Anwar *et al.*, 2017).

### **Adult learners and cybersecurity education**

Furthering the concern that the human factor is the weakest link in an organization’s security chain, researchers (Anwar *et al.*, 2017; Fatokun *et al.*, 2019; Olmstead and Smith, 2017) look at the role played by age on cybersecurity awareness. Jacob *et al.* (2019) discovered that “there has also been a significant growth in tech adoption in recent years among older generations” (p. 72), which was often driven by younger technology users in their lives. Research has shown that “people over 55 are overall not well educated when it comes to cybersecurity” (Ricci *et al.*, 2019, p. 231), they represent a generation less exposed to technology and currently some of the longer-standing employees within organizations. However, on the opposite side of the spectrum, we have “digital natives” otherwise known as Millennials who are

entering the workforce and are even more susceptible to cybercrime due to their lack of experience and overconfidence (Ford, 2021; Haney & Lutters, 2017; Redekop, 2021). While age plays a critical part in how an internet user uses the internet or reacts to cybersecurity incidents, education is an essential tool in the mitigation of many of the age-related issues stemming from a lack of cybersecurity awareness (Ricci *et al.*, 2019; Fatokun *et al.*, 2019).

Ricci *et al.* (2019) used the Pew survey conducted by Olmstead and Smith (2017) and further found that many adults “are unaware of key cybersecurity topics, terms, and concepts” (p. 244). They found that the key to developing an effective cybersecurity awareness program tailored to adults is important to identify what areas of cybersecurity they are most concerned with and would like to learn more about. As many organizations adopt new internet-based technologies, less tech-savvy adult employees may face issues of anxiety due to their lack of experience (Olmstead and Smith, 2017). Ricci *et al.* (2019) suggested that the combination of new technologies and an employee’s lack of experience can lead to a compromise in the organization’s security. Employee-sponsored or mandated cybersecurity awareness is critical to this augmentation of skills as many adults are less likely to partake in cybersecurity awareness training of their volition or on their own time, especially if it affects the primary work tasks (Ricci *et al.*, 2019; Chowdhury *et al.*, 2019; Yazdanpanahi, 2021).

### **Education Level and Cybersecurity Confidence**

Olmstead and Smith (2017) argue that regarding cybersecurity awareness, “most consistent differences are related to educational attainment” (p. 7). In their survey conducted for Pew Research, they found that “higher levels of education and younger internet users are more likely to answer cybersecurity questions correctly” (p. 7). The suggestion that internet users with higher levels of education attained are more aware of cybersecurity concepts is echoed by several

researchers (Ricci *et al.*, 2019; Costa *et al.*, 2019; Kostyuk and Wayne, 2020; Diaz *et al.*, 2020).

While other researchers argue that cybersecurity should be integrated with formal education (Zwilling *et al.*, 2020; Krishna and Sebastian, 2021; Catota *et al.*, 2019; Kweon *et al.*, 2019).

While education and the level of education attained an important demographic factor, cybersecurity education is a targeted response to a common ailment in multiple industries (Fatokun *et al.*, 2019). However, it must be noted that cybercriminals who participate in cybercrimes including but not limited to social engineering, phishing scams, and ransomware do not discriminate against a person's age, gender, or educational level attained.

### **Industry Perception of Cybersecurity Threat**

Costa *et al.* (2019) argue that while it is important to assess knowledge and awareness, it is also important to assess human behavior “in order to perceive the security risks we are currently facing as a society, governments, companies, etc.” (p. 2032). How individuals and organizations perceive the problem posed by cyber threats, can be a representation of how they prepare. Chowdhury *et al.* (2019) further that many “tend to perceive the costs... of meeting cybersecurity requirements as much higher than the expected benefits” (p. 1298). Fatokun *et al.* (2019) suggest that these failures to perceive the threat posed by cybercrime and prepare accordingly, are also rooted in the previously discussed demographic characteristics, including notions such as perceived vulnerability and perceived severity of cyber threats. Enhancing the cybersecurity awareness of individuals helps them to properly understand the threats associated with cybercrime and improve an organization's mitigation efficacy and perceived vulnerability.

### **Cryptovirology: The Rise of Ransomware**

Cryptovirology, a type of malware, now simply known as ransomware is a formidable threat affecting many organizations, “attacks make the news daily” (p. 26). Young and Yung

(2017) explain the origins of ransomware and suggest that many horrible things were designed by accident. The authors refer to ransomware as the “unholy union” (p. 24) of cryptography and malware. The designers wanted to know how devastating and malicious a software attack could be on a proposed target. Zimba *et al.* (2019) explain that “the incorporation of encryption into malware has given birth to new forms of cyber-attacks the most notable being cryptoviral extortion” (p. 3259). They created an evolved malware that could not be forcefully removed. Essentially an attacker encrypts the victim’s data and demands a usually significant ransom amount (paid in cryptocurrency) before returning access to the encrypted data. Furthermore, the advent of ransomware has “changed the very definition of ‘computer breach’” (Young & Yung, 2017, p. 26), now organizations need to contend with the possibility of extortion and data exfiltration. This has led to many federal, state, and local government agencies introducing laws and penal codes to legitimize cybercrime and outlaw the use of ransomware as well as mandate the education of computer users (Yazdanpanahi, 2021; Macmanus *et al.*, 2013; Kortjan and Solms, 2014; Kessler and Ramsay, 2013; Skertic, 2021).

Several authors further explain how a crypto-viral attacker uses public and private encryption keys to encrypt data and only offers the decryption key when the ransom is paid (Zimba *et al.*, 2019; Young and Yung, 2017; Salunke *et al.*, 2021). Payment only exacerbates the situation and motivates would-be attackers, and possibly funds terrorist organizations, however, it is often the only solution for most organizations (Skertic, 2021; Costa *et al.*, 2019; Young and Yung, 2017; Chung, 2019). Furthermore, Young and Yung (2017) state that the ransomware “business model” used today, is a billion-dollar cybercrime industry (p. 25). Moreover, Young and Yung (2017) reveal that 20+ years ago, they posited that weaponized cryptography would be the world’s top cyber threat and even went as far as suggesting countermeasures, but their

warning fell on deaf ears with many security professionals dismissing and disregarding the warning. Many dismissed the notion that cybercrime was a real threat, for most organizations and technology departments, cybersecurity, as a result, is often an afterthought, usually after a compromise (Young and Yung, 2017; Costa *et al.*, 2019; Kessler and Ramsay, 2013).

Organizations need every advantage to combat the threat of cryptoviral extortion (ransomware) attacks and the least costly involves their first line of defense, an educated and cyber-aware workforce (Oancea *et al.*, 2019; Zwilling *et al.*, 2020; Tirumala *et al.*, 2019; Daengsi *et al.*, 2021).

### **Understanding The Gap Between Perceived Threats to and Preparedness for Cybersecurity**

The internet opened a wealth of knowledge to the world, unfortunately, it also “brought about an unprecedented level of vulnerability” (Nam, 2019, p. 1). de Bruijn and Janssen (2017) state that “cybersecurity can be perceived as a problem of the individual or as a problem of society” (p. 4). The internet has also given rise to cyber-terrorism, which has shaken the “social faith in governments and corporations” (Nam, 2019, p. 1) capabilities to assess risk and prevent future attacks. Kostyuk and Wayne (2020) further argue “that citizens do not see data breaches as a major threat because these threats are perceived as less common” (p. 4). Cybercrime and cyber-terrorism affect individuals and organizations alike, their perception of these threats determines how they prepare for them, determining the likelihood of surviving the attack (Fatokun *et al.*, 2019; Chowdhury *et al.*, 2019; Nam, 2019).

Nam (2019) used data collected from a Pew Research Center survey conducted in 2016, specifically looking at the relationship between the perception of a cybersecurity threat and the preparedness for that perceived threat. Nam was looking for the psychological impact (intent to

act) created by the threat of cyber-terrorism and how cybersecurity awareness narrows the gap between perception and preparedness to lower organizational vulnerability, by drawing attention to security issues and raising confidence. Zwilling *et al.* (2020) further explained that “perception of situations is subject to control due to individual knowledge increases motivation to act” (p. 10). However, that enhanced confidence can also lead to less preparation, whereas feelings of insecurity lead to over-preparation (Kortjan and Solms, 2014; Fatokun *et al.*, 2019; Kostyuk and Wayne, 2020).

Nam (2019) found that “cybersecurity awareness...increased recognition of vulnerabilities” (p. 7) is similar to the way that past experiences (experiential) with cybersecurity breaches increase awareness. That several psychological constructs including but not limited to cognitive awareness dictate how an individual or organization will actively prepare for a cyberattack as opposed to allowing fear (psychological) and anxiety (emotional) to drive their response (Kostyuk and Wayne, 2020; Nam, 2019; Chowdhury *et al.*, 2019). Nam (2019) recommends that in the inevitability of a cybercrime incident organizations, especially government agencies should work to “further enhance their efforts by strengthening awareness training and security behavior” (p. 9). A cyber security-aware workforce allows education and experience to “influence the level and type of perceived preparedness relative to the perceived threats to cybersecurity” (p. 9). Cybersecurity awareness in the workforce allows for a more effective preparedness response to cyber-terrorism, a response that is more likely to result in a favorable ending (Catota *et al.*, 2019; Ricci *et al.*, 2019; Kweon *et al.*, 2019; Skertic, 2021).

### **Cybersecurity in Local Government**

Local government needs to contend with two conflicting principles when considering cybersecurity, one is the right of the people to open government called *transparency*, and the

second is avoiding measures that can violate public values such as privacy (Macmanus *et al.*, 2013; Yazdanpanahi, 2021; de Bruijn and Janssen, 2017). Macmanus *et al.* (2013) further suggest that cybersecurity adds to the complexity of government agencies having to protect their organization's infrastructure and subsequently the data of their constituents. The state that "fear of cyberattacks" is driving the development of new "policies and procedures" at the local government level, but often with the same insufficient funding that is also commonly associated with local government (Macmanus *et al.*, 2013, p. 452). Yazdanpanahi (2021) furthers that state-level government is intervening through mandated training and policy that "will create a strong security culture that can go a long way toward minimizing threats for city government" (p. 4). Furthermore, Macmanus *et al.* (2013) suggest that many members of the public "fear that their privacy rights will be diminished" (p. 453), if the government has to raise its security level as breaches of government networks increase and concerns about their private data being at risk are also increasing. Moreover, the advent of E-government means that local government agencies are providing more services online, which while generating additional revenue and providing a facility of transparency to its constituents, also requires improved security measures on the part of the government, which could effectively reduce access (Conklin and White, 2006; Macmanus *et al.*, 2013).

For government entities, the absence of a continual push for cybersecurity awareness can be attributed to various factors, such as an unforgiving political and media environment when errors are made concerning the reliability of the information or the security of sensitive content, the limited fiscal budgets appropriated to technology departments (MacManus *et al.*, 2013; Krishna and Sebastian, 2021; Conklin and White, 2006). Nam (2019) furthers that there is also a psychological factor between the perceived and potential cyber threats the organization faces



that also affects the push for cybersecurity awareness. The demand for transparency from the public is two-fold for employees of local government, whose employment is contingent on a request for transparency that infringes on their privacy. The reduced expectation of privacy is further exacerbated by cyberattacks with a political agenda (de Bruijn and Janssen, 2017; MacManus *et al.*, 2013; Skertic, 2021; Kostyuk and Wayne, 2020). This creates the studied cross-pressure on government agencies to both provide and secure information. Nam (2019) suggests that “clearer standards and procedures with regard to how to provide cybersecurity as well as better training” (p. 466), help balance the demand for transparency and privacy.

### **Motivational Factors Influencing Cybersecurity Intent to Act**

Baier (1970) states that intent to act can only occur if it is “something we can intend, it must be something we can do, not just something that we do; that is, we must be able both to do it and not to do it” (p. 657). Furthermore, employee behavior and resultant actions are often influenced by different factors within their employing organization, including the perceived importance of cybersecurity and the resultant business continuity (Chowdhury *et al.*, 2019). Zwilling *et al.* (2020) suggest that these factors can help motivate employees to behave in a certain way, and that “perception of situations as subject to control due to individual knowledge increases motivation to act” (p. 10). The literature further shows that management intervention and support drive many of the behavioral aspects of an organization including but not limited to cybersecurity culture and awareness (Krishna and Sebastian, 2021; Yazdanpanahi, 2021; Kortjan and Solms, 2014; Costa *et al.*, 2019). Management interventions including training, prepare the employee to act in the face of a potential cybersecurity compromise (Chowdhury *et al.*, 2019; Kweon *et al.*, 2019; He *et al.*, 2019). Baier (1970) argues that a person can not intend to do something they do not know how to do, they must learn to do it first. Therefore, the application

of cybersecurity training could provide the knowledge required for an employee to act accordingly under cybersecurity threat scenarios.

### **Skills and Successful Cybersecurity Advocacy**

How an organization perceives and prepares for cybersecurity threats depends greatly on how the message is presented to the organization. Spremić and Šimunic (2018) present the idea that organizations “still assume cyber security is solely the responsibility of IT departments or assigned individuals” (p. 345). While other authors have presented that cybersecurity is a problem that spans the organization, insisting that employees and management should be equally involved (Yazdanpanahi, 2021; Catota *et al.*, 2019; Ricci *et al.*, 2019; Kweon *et al.*, 2019; Skertic, 2021). The designated individuals responsible for cybersecurity awareness within an organization, require specialized skills to contend with a lack of cybersecurity awareness and technical skills in their organization’s employees. Regarding the specific skills, Dawson and Thomson (2018) further “argue that the people who operate within the cyber domain need a combination of technical skills, domain-specific knowledge, and social intelligence to be successful” and further that some of these skills are not something someone can simply be trained on (p. 1). This results in many organizations lacking “the right personnel to communicate cyber threats to less technologically savvy decision-makers” (Haney & Lutters 2017, p. 3) in management and subsequently the organization’s staff.

Haney and Lutters (2017) argue that designated cybersecurity staff referred to as “cybersecurity advocates” must have the necessary technical skills (credibility) to understand the underlying threat but also “possesses the ability to promote best practices, educate, persuade, and serve as change agents for cybersecurity adoption” (p. 1). These advocates serve as ‘translators’ for the organization to bridge the gap between the technical and social aspects of cybersecurity.

When working with non-tech savvy employees it is soft skills like communication and empathy that makes these advocates successful in conveying cybersecurity best practices as well as training to members of the organization. While this combination of technical and social skills is crucial for these advocates to spread their message, a later study by Haney and Lutters (2021) referred to them as additionally playing the role of “force-multipliers in security adoption” (p. 497). These advocates fulfill this role by helping their organization’s staff with cybersecurity awareness education and best practices, effectively making the rest of the organization extensions of the organization’s security team.

### **Safer Practices to Enhance Cybersecurity in Government**

The dependency on digital data for the government and its constituents has increased the need for those organizations to make every effort to safeguard this digital resource. Phishing attempts are a common method used to compromise these organizations’ users and allow cybercriminals to gain access to these digital resources. Ikhsan and Ramli (2019) suggest that “employees are the closest to restricted government information” (p. 1) and further suggest that these employees must have security awareness for the overall security of the organization. Cybersecurity awareness is an important tool in safeguarding digital information, being able to apply conscious thought before acting on a phishing e-mail (Think Before You Click) can save an organization from a serious compromise (Costa *et al.*, 2019; Peker *et al.*, 2016; CISA, 2020).

Organizations like CISA and other researchers have started to suggest additional practices to be included in and to complement cybersecurity awareness training (CISA, 2020; Weber *et al.*, 2008; Matthews, 2012; Walsh, 2020). Phishing attempts have become more effective and more aggressive and additional safeguards including but not limited to stronger passwords and multi-factor authentication make it more difficult for a cybercriminal to

compromise government employees (Ikhsan and Ramli, 2019). Weak, simple, or easily guessed passwords can be obtained in a phishing campaign or through social engineering methods (Weber *et al.*, 2008). Cybersecurity awareness training helps educate users on safer internet identity protection practices and helps reduce the threat caused by employees who lack cybersecurity awareness and best practices to safeguard their online identities against the “various social engineering techniques used to manipulate, influence, and deceive government employees” (Ikhsan & Ramli, 2019, p. 2).

### **Summary**

This chapter presented an overview of the literature surrounding the relevant issues in cybersecurity and how organizations prepare to be more cybersecurity aware. Also, it introduced the theoretical framework. Chapter Three will present the methodology that was used to address the research question proposed in this study.

## CHAPTER III

### RESEARCH METHODS

#### **Introduction**

]The purpose of this study was to analyze the effect of a cybersecurity awareness training program on government employees' knowledge of cybersecurity issues and their ability to mitigate cybersecurity threats was explored using the following research hypotheses:

- There is a statistically significant positive effect of a cybersecurity awareness training program on government employees' knowledge of cybersecurity issues and practices as measured by a comparison of their pre-and post-test scores.
- There is a statistically significant positive effect of a cybersecurity awareness training program on government employees' ability to mitigate cybersecurity threats as measured by the frequency of mitigated cybersecurity threats identified prior to and after the training
- There is a statistically significant relationship between employees' cybersecurity awareness scores and demographic variables such as gender, age, and the highest level of education attained.

This chapter includes the following sections: Research Design and Methodological Rationale; Participants; Instrumentation; Treatment, Data Collection Procedures; and Data Analysis Procedures.

## **Research Design and Methodological Rationale**

To satisfy the objectives of the research hypotheses, a quantitative research approach was used, which included archival data from the Cameron County's Information Technology Department from their cybersecurity training and assessments. This was part of the County's adoption of an annual state-mandated cybersecurity training program and a cybersecurity awareness survey.

The risk presented by a cybersecurity compromise made it not possible to conduct an experimental study as the data were archival and all members of the target group were required to take the training. The House Bill 3834 mandate required the inclusion of supervisors and elected/appointed officials to be included in addition to frontline employees. The mandatory nature of the requirements ensured that the government employees took part in the training and took the pre-post-test surveys. All qualified county employees were provided with the survey questionnaire which was used to assess their cybersecurity knowledge and awareness.

## **Participants**

Cameron County is geographically located at the southernmost tip of Texas and had an estimated population of 423,163 at the time of the study. Cameron County government at the time of this study had a workforce count of 1200, of that number, 1024 participants (85%) met the requirements and participated in the security training required by the County. The mandate stated that only computer-using employees or those who work at the computer at least 25% of the time were required to participate in the training. The demographic data presented in Tables 1 and 2 below present a breakdown of the County employees who participated in the training, based on the variables of gender, age, and the highest level of education. The participating employees consisted of 54.3% female employees and 44.8% male employees. Where the

majority of the employees 30%, ranged in age from 36 to 45, followed by 26% at 46 to 55 years and 25% from 26 to 35 years of age. The highest education level attained was another demographic collected as that technology and education are sometimes related. More than half of the participating employees 52% possessed a High School level education, followed by 16 % holding an Associate degree, 20% holding a Bachelor's degree, and only 10% holding a Master's degree or higher.

Table 1: Gender and Age

		<b>Age Range by Gender</b>					<b>Total</b>
		<b>18 to 25</b>	<b>26 to 35</b>	<b>36 to 45</b>	<b>46 to 55</b>	<b>56 and older</b>	
	<b>Male</b>	27	117	119	118	78	459
	<b>Female</b>	38	133	182	147	56	556
	<b>Prefer not to answer</b>	0	4	1	2	2	9
<b>Total</b>		65	254	302	267	136	1024

This study required the systematic analysis of archival data for the target group of existing local government employees working in Cameron County's local government during the organization's annual response to a state-mandated cybersecurity training, which is in fulfillment of The Texas Legislature's House Bill 3834. All employees who participated in the required training used a computer at least 25% of the time to complete their daily work and were therefore required to take the annual cybersecurity training.

Table 2: Gender and Education

	H.S. Diploma / GED	Highest Educational Degree held					Total
		Associates	Bachelors	Masters	Doctorate	Not applicable	
Male	261	61	72	26	30	9	459
Female	271	100	131	22	20	12	556
Prefer not to answer	1	0	1	2	3	2	9
	533	161	204	50	53	23	1024

The archival survey data used as part of this study also included information regarding how employees rated their technical knowledge. Please see Figure 6 below.

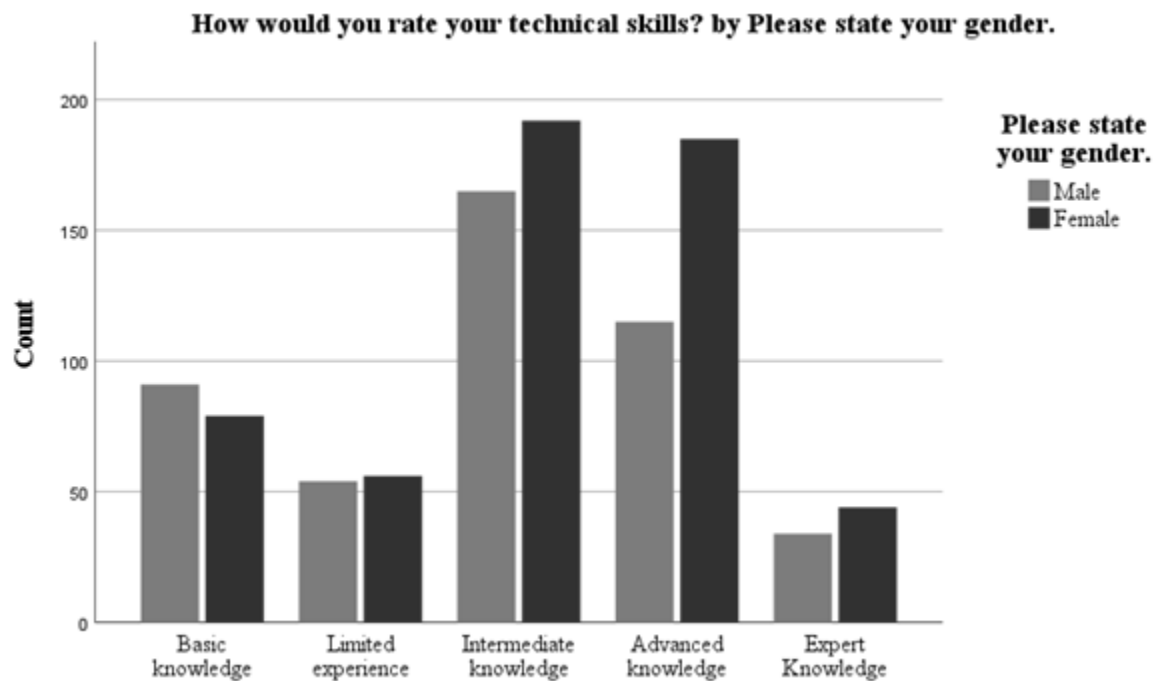


Figure 6: Self-Assessed Technical Skills by Gender



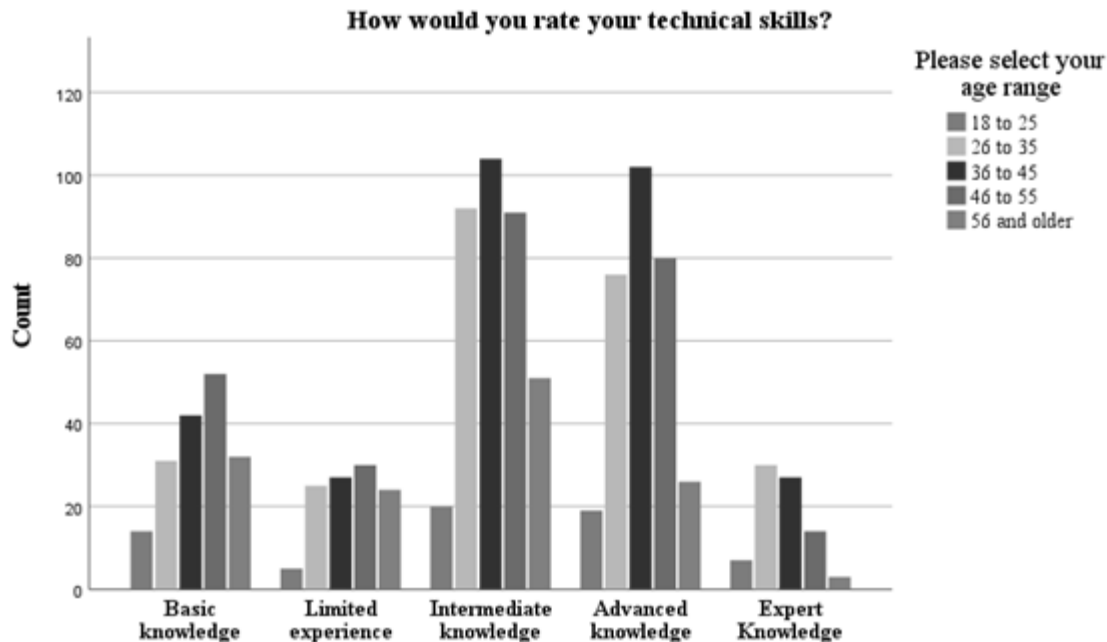


Figure 7: Self-Assessed Technical Skills by Age Group

Moreover, the employees who participated in the training, consisted of the majority if not the entire workforce to maintain the integrity of both the organization and the participants in the event of a cybersecurity-related incident.

### Cybersecurity Program

The Cameron County Information Technology Department is responsible for the cybersecurity defenses of the County including but not limited to cybersecurity education and assessment. The approval of House Bill 3834 and the subsequent House Bill 1118 mandated that the organization provide approved cybersecurity training on an annual basis or be disqualified from most state and federal grants. The training consisted of short videos and assessment questions to ensure understanding of the concepts. The training was reinforced using mock phishing tests, the controlled use of the same deceptive tactics used by cybercriminals to trick

employees into causing a compromise. Their assessments use random sample sizes and samples of the population to gain insight into the existing level of cybersecurity awareness.

### **Instrumentation**

In this study, archival data were obtained from existing survey results and mock phishing tests conducted by the Information Technology Department. The data were analyzed to determine if there were any significant statistical differences between pretest and post-test responses as a result of the cybersecurity training and if any demographic factors had a role in the improvement or understanding of cybersecurity concepts and safer internet practices.

### **Cybersecurity Knowledge Survey**

The survey used by Cameron County was adapted from Pew Research's Cybersecurity Knowledge Quiz (Smith, 2017) and contained the following constructs: Secured internet browsing (SB), Virus infection (VI), Phishing (PH), Botnets (BN), Multi-Factor Authentication (MFA), Passwords (PS), Ransomware (RN), Internet Privacy (IP), GPS Tracking (GPS), Virtual Private Networking (VPN), and Wireless Safety (WS). Pew Research Center's (2016) Cybersecurity Knowledge Quiz was developed to evaluate cybersecurity awareness in the American population. It was first deployed in 2017, to assess what the U.S. public knows about cybersecurity. The authors of this survey Olmstead and Smith (2017) investigated why "many Americans do not trust modern institutions to protect their personal data – even as they frequently neglect cybersecurity best practices in their own personal lives" (p. 2). The technical questions which were taken from the Pew Research survey consisted of eleven multiple-choice questions to assess the employees' existing knowledge of cybersecurity concepts and mitigation efforts. Cybersecurity is a complicated subject, however, the questions included in the survey

cover many of the general concepts that cybersecurity professionals stress are critical for users to protect themselves while conducting their digital lives.

The multiple-choice questionnaire included in the survey was aligned with Bloom's Taxonomy and the learning outcomes of remembering, understanding, and application were used to assess the target group before and after the mandated training. Cybersecurity not only requires the knowledge and understanding of cybersecurity concepts but also the ability to recognize the tactics of cybercriminals when an attempt to compromise them or their organization is made. This questionnaire allows for measurements at levels 1 (remembering), 2 (understanding), and level 3 (applying) of Anderson-Krathwohl's revision of Bloom's Taxonomy (Wilson, 2016).



Figure 8: Bloom's Taxonomy (Halawi *et al.* (2009))

The usability of Bloom's taxonomy was furthered by Halawi *et al.* (2009) who stated that "Bloom's taxonomy was developed so that researchers could categorize the objectives of the learning system" (p. 374). A learning system that was developed by the Information Technology Department and inclusive of the cybersecurity course that these employees took as part of the mandated H.B. 3834 response that addresses levels 1 and 2 of Bloom's taxonomy and the mock

phishing tests that addressed level 3, application. The survey was used to determine to what degree the employees understood the presented cybersecurity concepts and then applied them to not only their responses in the questionnaire but while accessing the internet. The analysis of the archival pre-and-post-survey assessment data was used to understand the effectiveness of this cybersecurity awareness training program. The Pew questionnaire was designed to understand the extent to which a population understands cybersecurity concepts, the first iteration was conducted on the American public (Olmstead and Smith, 2017). The instrument included several common cybersecurity concepts including:

- Securely accessing the internet via browsers and public Wi-Fi;
- Attempts at compromise like phishing attacks and malware;
- Secure passwords;
- Two-Factor authentication to better protect themselves online;
- Ransomware and its effects on organizations;
- And securely remote accessing their company's network.

### **Demographics Survey**

The survey questionnaire used by the County included ten questions designed to collect demographic and employment data for the target group. The following demographic variables were included: Time with the organization (YR), Ethnicity (ET), Gender (G), Age (AG), Education level (ED), Primary Language (PL), Technical Self-efficacy (SE), and Department (D). This was included by the organization to collect employment and demographic data from Cameron County's employees. The digital survey was administered by Cameron County's Information Technology Department via the organization's E-mail system and using SurveyMonkey® as their data collection platform. The government employees received the

survey as part of the organization's mandated response to Texas House Bill 3834, which required them to partake in cybersecurity training. It was used to measure an employee's ability to understand cybersecurity concepts, apply pertinent content to their daily operations, and recognize tactics used by cybercriminals to compromise organizations.

The archival data collected by these instruments provided insight into psychological, social, demographical, and educational factors that may be affecting these government employees' cybersecurity behaviors. Olmstead and Smith (2017), conducted the original survey for Pew Research which determined that older generations are usually less aware of cybersecurity concepts when compared to younger subjects, and subjects with higher levels of education were a good indicator of having more awareness of cybersecurity concepts. Anwar *et al.* (2017) furthered the demographic discussion by suggesting that gender also was a factor that affected cybersecurity beliefs and behaviors. The demographic portion of the survey collected the following demographics (See Appendix A):

- Years working at the organization;
- Ethnicity;
- Gender;
- Age;
- Highest Educational Degree Held;
- Primary Language;
- How they rate their technical skills;
- Their department within the organization;
- Previous Cybersecurity training.

Analyzing the archival data will provide a clearer understanding of the effect of the cybersecurity training population along with any effects related to the other measured constructs. Cameron County conducted this assessment to understand its current security posture, and the results would add to the improvement of future cybersecurity exercises provided to its employees regarding cybersecurity concepts with efforts to improve their security posture.

### **Data Collection Procedures**

Following approval from Cameron County Administration and the Institutional Review Board of The University of Texas Rio Grande Valley, archival data were obtained from the Cameron County Information Technology Department for all employees who took the mandated cybersecurity training in 2021. The Information Technology department used the web-based SurveyMonkey as their survey platform to administer the online surveys, a sample is included in Appendix A. The participants were required to have an organization-provided e-mail address to receive and participate in the survey that was included with the training course. The online survey collected general demographic details and existing knowledge related to cybersecurity and safe internet practices before and after the provided training course. The included demographic details consisted of gender, age, race, education, department, and the current length of employment with the organization. The survey was adapted from a Pew Research survey (2017) to determine the users' level of understanding of cybersecurity concepts and their respective scenarios.

The online survey was included with the required training e-mail, as part of the dissemination. The link and/or a QR code was provided to the participant to access the questionnaire via their computers or mobile device. The survey results were collected online by

the organization. The collected archival data were processed and analyzed using the methods described in the next section.

### Data Analysis Procedures

To address the first research question, data collected from the pre-and-post-survey questionnaires were analyzed to determine if there is any statistical significance in the pre-and post-survey scores. Peker *et al.* (2016), also looked for statistical significance in their study where they also looked at the cybersecurity awareness of their population and wanted to understand the effectiveness of security awareness programs by looking for a statistically significant increase in post-test scores. Peker *et al.*'s study determined that the cybersecurity awareness program “has raised their level of awareness not only for the specific topics that the module addressed but overall, in cybersecurity” (p. 15). This statistical test helped determine if there was a significant effect on cybersecurity awareness in our population because of the implementation of cybersecurity training.

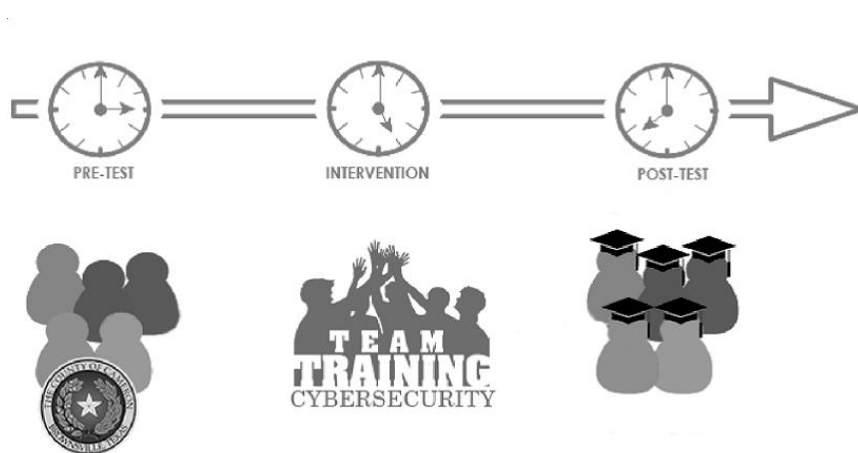


Figure 9: Analysis of variance across time

Their study required the comparison of the changes in mean scores over time, analyzing the data using repeated-measures ANOVA (Analysis of Variance). The repeated measures ANOVA tests for whether there were any variances between related population means. Two separate points (pre-intervention and post-intervention) were analyzed for statistical significance in the final test scores. This particular test required one independent variable and one dependent variable. The dependent variable was the cybersecurity training offered annually and the independent variable was the repeated measurable test scores. The measurements were repeated over time, by measuring changes in resultant test scores as a result of the cybersecurity training program.

The second question assessed the change in the mitigation skills of employees through a series of mock phishing attempts conducted by the Cameron County IT department. These phishing attempts were conducted randomly on a random sample of the population, it was important to note that these population samples may not have been representative of the entire population. The phishing tests were used to determine whether employees who had taken their mandated training were still susceptible to attempts made to compromise the organization. The assessment collected which employees ignored, clicked links, opened attachments, or entered personally identifiable information (PII) into a phishing website. Each level was more critical to the security compromise of an organization. The analysis of the archival data looked for the changes in percentages over some time which included before the mandated training and included phishing attempts that had taken place after the required training.

To assess the third research question, a regression analysis was conducted on gender, age, the highest educational level attained, and how they self-assess their technical skills, to identify any significant differences to post Cybersecurity Knowledge Survey assessment scores. The



regression analysis of the demographic variables helped to identify statistically significant relationships between their collected variables and the results of cybersecurity training. Diaz (2020) used Pearson's R and Cramer's statistical tests to look for relationships between demographic factors and a population click rate on phishing e-mails, another studied cybersecurity attack method. Anwar *et al.* (2017) studied the gender differences in cybersecurity behaviors through an online survey and found no significance ( $p = 0.248$ ) between gender and cybersecurity behaviors, but there were significant gender-based differences in technology adoption and perception of risk. Ricci *et al.* (2019), also conducted a survey-based study on age and cybersecurity awareness education courses and found that the vast majority of participants were interested in cybersecurity education where age-related changes in ability were taken into account when designing products and training programs for aging adults (p. 245).

### **Limitations of the Study**

This study was delimited to a population of local government employees in South Texas, who had been provided with state-mandated cybersecurity awareness training that should have been completed by June 14<sup>th</sup>, 2021. The course was required by the Texas State Legislature, following House Bill 3834 which was passed on April 25, 2019. The training was required of local and state government employees and even state contractors who use a computer to complete at least 25 percent of the employee's required duties.

### **Prior Exposure to Cybersecurity Awareness Content**

Due to the number of mock phishing attempts that had been conducted by the Information Technology Department's Security team, that lead up to the annual observation, employees may have had a greater awareness of cybersecurity concepts and topics ahead of the survey and state-mandated training. This study also took place during the newly-minted history

related to the SolarWinds hack (Jibilian and Canales, 2021) and more recently the Colonial Pipeline hack (Oxford Analytica, 2021) where terms like cyber-compromise and ransomware were being explained to the general public. Which may have swayed the awareness of the target group.

### **Phishing Test Data**

Phishing attempts made by the IT department's security team were random and the sample size was also random. Results were considered as an approximation and best effort to determine whether the population remained susceptible to cybersecurity compromise after the application of training.

### **Limitations related to one-group quasi-experimental research design with pre-and post-test Research**

A limitation of a one-group quasi-experimental research design was that a participant cannot receive the treatment condition first and then be tested in an "untreated" control condition. Participants in the study could have taken the assessments in the wrong order or both at the same time, therefore, affecting the results. Participants may have been exposed to other cybersecurity content before the treatment or discussed the assessment with other employees, which may have affected the way in which they answered the pre-and post-test survey.

### **Limitations related to survey research**

A limitation of survey research in our study is that there was likely a lower priority for partaking in the survey because of competing urgent tasks. Employees may have left questions unanswered, due to a lack of understanding and interpretation. While House Bill 3834 has a set requirement for government employees, there was a lack of enforcement and enforceable repercussions at the state and local levels, and some employees may not have participated.

Some participants may have felt uncomfortable providing answers that present them or their internet practices in an uncomplimentary manner. Other participants may simply be going through the motions and therefore not feel encouraged to provide correct, honest answers.

### **Limitations related to the Covid-19 pandemic**

A limitation in the collection of data during the covid-19 pandemic, no archival phishing data was collected or available for the year 2020 due to circumstances related to working from home and alternating schedules for the studied population.

### **Validity and Reliability of the Survey Instrument**

In regards to the validation of the instrument, the results of Pew Research's 2016 survey were referenced in studies by Black *et al.* (2018), Kostyuk and Wayne (2020), and Ricci *et al.* (2019), and Olmstead and Smith (2017). Pew Research's ethics statement implies that they only use tools and methods of analysis that in their professional judgment permit external parties to evaluate the credibility of their results. The adapted instrument used by Cameron County was reviewed by the Chief Information Security Officer of the government agency to help establish face validity and ensure that the instrument measures what it was designed to measure, the existing (or improved) cybersecurity awareness of the participant government employees.

### **Extraneous Variables**

Another limitation of the study would include existing employee awareness of cybersecurity concepts due to ongoing campaigns by the IT department regarding the cybersecurity of the organization, including the House Bill 3834 Mandate in the Spring and the NCSAM observation in October. In recent years news and social media have brought cybersecurity compromises to government agencies and critical infrastructure. These include but are not limited to Facebook (2019), City of Atlanta (2018), City of Baltimore (2019), Solarwinds

(2021), Colonial Pipeline (2021), and T-Mobile (2021). There was no attempt made to verify to measure how honestly or accurately the participants completed the demographic portion of the survey. While the survey was included as part of addressing the House Bill 3834 mandate, some participants may not have seen the invitation because they were working out on the field or deleted one of the requests accidentally.

### **Summary**

This chapter presented the Methodology section of the research proposal, which was used to achieve the purpose of the study. Chapter Four presents the results produced by these procedures.

## CHAPTER IV

### RESULTS

#### **Introduction**

The purpose of this study is to analyze the effect of a cybersecurity awareness training program on government employees' knowledge of cybersecurity issues and their ability to mitigate cybersecurity threats. Therefore, the study addresses the following research questions:

- What is the effect of a cybersecurity awareness training program on government employees' knowledge of cybersecurity issues and practices?
- What is the effect of a cybersecurity awareness training program on government employees' ability to mitigate cybersecurity threats?
- What demographic factors are related to government employees' knowledge of cybersecurity issues and practices and their ability to mitigate cybersecurity threats?

This chapter describes the results that were obtained when the different hypotheses were tested using the methodology described in the previous chapter. The results are reported in tabular, graphical, and descriptive formats.

## Results Summary

The Cameron County cybersecurity training included a pre-test and post-test to measure the effectiveness of the training. While the completion of the training meets the requirements mandated by Texas House Bills 3834 and 1118, there is still a viable concern that the training may leave them susceptible to a user-based cybersecurity compromise.

### Results Obtained for Research Hypothesis One

To test the first research hypothesis, there is a statistically significant positive effect of a cybersecurity awareness training program on government employees' knowledge of cybersecurity issues and practices as measured by a comparison of their pre-and post-test scores, a repeated-measures ANOVA (Analysis of Variance) was performed to compare the effect of cybersecurity training on the employees of the Cameron County government. The Qualified Target group (N = 1024) of Cameron County government employees took the pre-test, mandated cybersecurity training, and post-test. The resultant descriptive statistics are listed in the table below:

Table 3: Descriptive Statistics

<b>Descriptive Statistics</b>			
	<b>Mean</b>	<b>Std. Deviation</b>	<b>N</b>
<b>Pre-Test Score</b>	68.41	19.43	1024
<b>Post-Test Score</b>	82.02	16.23	1024
<b>Grand Mean</b>	<b>75.215</b>		
<b><i>Difference</i></b>		<b>13.61%</b>	

As shown in Table 3, the calculated Means for the pretest and posttest were 68.41 and 82.02, resulting in a 13.61% increase between assessments.

## **Results Obtained for Research Hypothesis Two**

To test the second research hypothesis, there is a statistically significant positive effect of a cybersecurity awareness training program on government employees' ability to mitigate cybersecurity threats as measured by the frequency of mitigated cybersecurity threats identified before and after the training, archival data from annual phishing campaigns conducted randomly over time by the Cameron County IT department were analyzed. While the pre-test and subsequent post-test results of the mandated cybersecurity training proved significant, the testing reflects that users can answer questions regarding their knowledge of cybersecurity issues and concepts. Knowledge of cybersecurity tactics and concepts is only a portion of an organization's cybersecurity posture and the path toward cyber resilience. Reinforcement of an employee's knowledge with real-world scenarios of cybersecurity concepts is a method of ensuring that internet users are not as easily compromised. To address the second question, archival data from annual phishing campaigns conducted randomly over time by the Cameron County IT department were analyzed. A phishing campaign is a series of fake e-mails sent to test a user's ability to identify and report suspicious e-mails as opposed to opening, clicking, and potentially causing a compromise. It is important to note that the participants studied were a random sample of the population and not indicative of the entire population. Phishing attempts were compared to determine if the training exerted any effect on government employees' ability to identify suspicious phishing emails and potentially mitigate an organizational compromise.

The attempts were made from October 2018 through June 2022 using different phishing systems, no testing phishing testing was conducted in 2020 due to operational changes as a result of the COVID-19 pandemic. The data collected for this study was from the 2021 mandated response to the HB 3834 cybersecurity training requirement.

Table 4: Phishing Campaign 2018

<b>2018 Campaign: Baseline Phishing Security Test – All Users</b>					
<b>Statistics</b>	<b>Recipients</b>	<b>Clicks</b>	<b>Attachment Opened</b>	<b>Data Entered</b>	<b>Phishing Reported</b>
<b>70.2%</b> Phish-Prone Percentage	<b>1180 (100%)</b>	<b>463 (45.21%)</b>	<b>0</b>	<b>365 (35.64%)</b>	<b>0</b>

In 2018, before the passing of Texas House Bill 3834 by the House on April 25, 2019, the Cameron County IT department conducted the first annual phishing campaign in observance of National Cybersecurity Awareness Month (NCSAM) in October. The Target group of the initial campaign in 2018 (N=1180) was sent a phishing e-mail requesting a password change. The results were that 463 employees opened the phishing e-mail and an additional 365 employees attempted to change their password using the provided phishing link. The results of this phishing campaign established that 70.2% of the employee target group could be compromised using a phishing e-mail. This phishing campaign was conducted before any official or mandated training was offered by Cameron County to its employees.



Table 5: Phishing Campaign 2019

<b>2019 Campaign: Baseline Phishing Security Test – All Users</b>					
<b>Statistics</b>	<b>Recipients</b>	<b>Clicks</b>	<b>Attachment Opened</b>	<b>Data Entered</b>	<b>Phishing Reported</b>
<b>19.4%</b> Phish-Prone Percentage	<b>1298 (100%)</b>	<b>146 (11.25%)</b>	<b>96 (7.40%)</b>	<b>9 (0.69%)</b>	<b>8 (0.62%)</b>

In 2019 after the initial H.B. 3834 mandated training course was provided in May; the next phishing campaign was also conducted in observance of National Cybersecurity Awareness Month (NCSAM) in October. The Target group of this campaign in 2019 (N=1298) was sent a phishing e-mail from Lone Star National Bank and included an attachment with a link. The results were that 146 employees opened/clicked the phishing e-mail, an additional 96 employees opened that attachment, and lastly, 9 employees entered banking data using the provided phishing link. The results of this phishing campaign showed a significant reduction in the employee target group from the previous year that could be compromised using a phishing e-mail, 19.4% were phishing prone. 2019 gave the Target group the ability to mitigate phishing attempts by allowing a single-click report button on their e-mail client. During this test cycle, 8 employees reported the phishing e-mail to IT.

Texas House bill 1118 was passed by the House on May 18, 2021, focusing on all state agencies and local government offices and their compliance with cybersecurity training requirements. Agencies that did not meet the mandated training requirement would lose access to grant funding. In 2020, while mandated training was conducted, no phishing tests were conducted due to operational changes (work from home) as a result of the COVID-19 pandemic.

Table 6: Phishing Campaign 2021

<b>2021 Campaign: Baseline Phishing Security Test – All Users</b>					
<b>Statistics</b>	<b>Recipients</b>	<b>Clicks</b>	<b>Attachment Opened</b>	<b>Data Entered</b>	<b>Phishing Reported</b>
<b>8.18%</b> Phish-Prone Percentage	<b>330 (100%)</b>	<b>8 (2.42%)</b>	<b>15 (4.55%)</b>	<b>4 (1.21%)</b>	<b>6 (1.82%)</b>

In 2021, the tool and method used to conduct phishing tests in Cameron County were replaced with a product from a company called Proofpoint. Phishing campaigns were conducted on smaller random groups within the Target group as opposed to the entire population and multiple campaigns were conducted. The new tool included a plug-in for the employee's Microsoft Outlook client that installed a button that would allow employees to identify and report phishing e-mails. The change in process and procedure was a direct result of the employees starting to return from the mandated COVID-19 protocol that had many of them working from home during the latter portion of the year. Which resulted in a significantly smaller Target group being tested. Table 4 reflects the combined results of the multiple phishing campaigns conducted in 2021. Two health insurance-related phishing e-mails were sent out in October and one streaming service-related in December 2021 to a smaller combined Target group (N=330) and saw a combined 2.42% of employees clicking/opening the e-mails, 4.55% opening the attachment, 4 (1.21%) employees clicked the link that would lead to a compromise, but more importantly 6 employees reported the phishing e-mail.

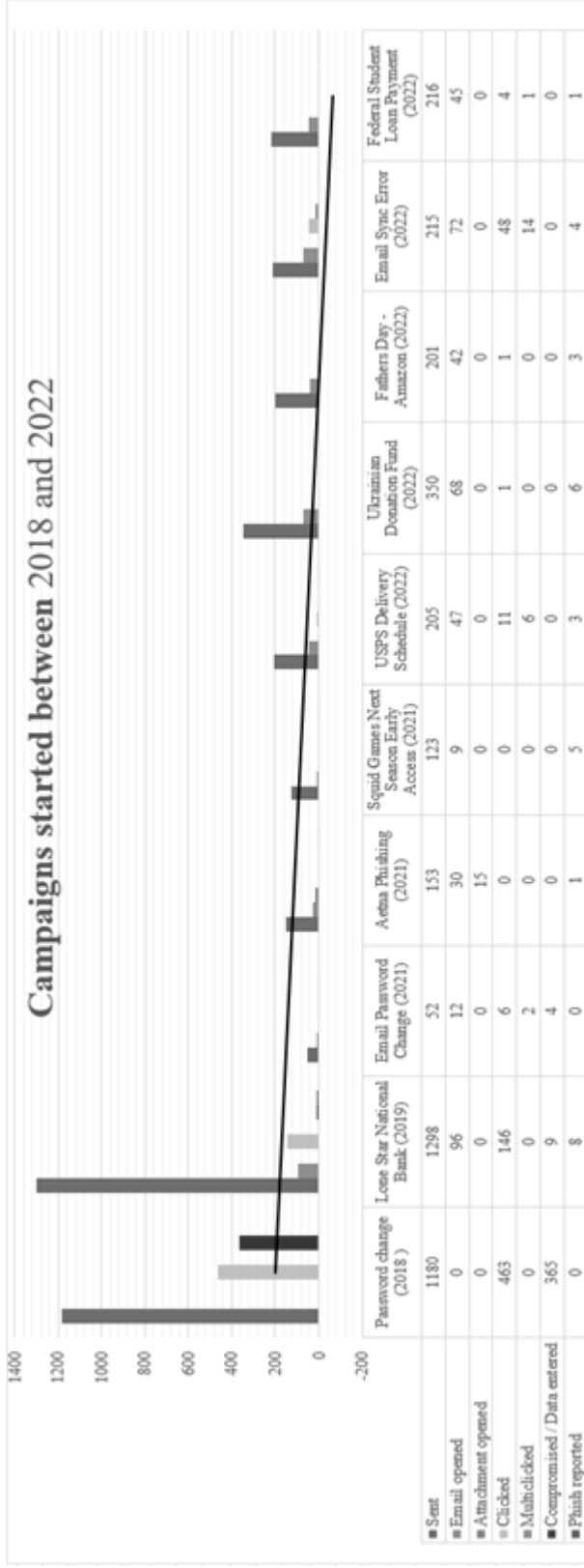
Table 7: Phishing Campaign 2022

2022 Campaign: Baseline Phishing Security Test – All Users					
Statistics	Recipients	Clicks	Attachment Opened	Data Entered	Phishing Reported
<b>30.33%</b> Phish-Prone Percentage	<b>1187 (100%)</b>	<b>86 (7.25%)</b>	<b>274 (23.08%)</b>	<b>0</b>	<b>17 (1.43%)</b>

A more aggressive set of phishing tests began in 2022, with them being issued in January, March, June, and two tests issued in October. 2022 reflected a higher percentage of employees being phish-prone, this is a direct result of new tools and using phishing topics that would lure employees into a false sense of safety. The security team at Cameron County used current events as topics for their campaigns, including but not limited to the War in Ukraine, an E-mail error, and the Federal Student Loan Forgiveness program that many public servants were applying for. It is this same false sense of safety that allows cyber-criminals to breach the “human firewall” (Diaz *et al.*, 2020; Chowdhury *et al.*, 2019).

These tests reflected a combined Target group (N=1187) and saw a combined 7.25% of employees clicking/opening the e-mail that would lead to a compromise, 23.08% opening the attachment, and 17 (1.43%) employees reporting the e-mail to IT. However, it was the 30.33% phishing prone that was concerning as it was almost an 11% increase from the campaign in 2019.

Figure 10: Phishing Campaigns in 2018-2022 with click trend



While the results appear consistent across the phishing campaigns, the graph presented in Figure 10 reflects that the click trend decreased across the phishing campaigns. Employees clicking on links and attachments are one of the leading causes of organizational compromise, a lowering click trend can improve an organization's security posture.

### **Results Obtained for Research Hypothesis Three**

To test the third research hypothesis, there is a statistically significant relationship between employees' cybersecurity awareness scores and demographic variables such as gender, age, the highest level of education attained, and their ability to mitigate cybersecurity threats, a multivariate analysis was used to analyze the relationship between the demographic variables and the scores on the cybersecurity pre-test and post-test.

The pre-test and subsequent post-test results of the mandated cybersecurity training were significant in reflecting that users can answer questions regarding their knowledge of cybersecurity issues and concepts. Increased training over time has shown a decrease in how prone the Target group is to be phished by a threat-actor and leading to a greater compromise of the organization. The collection of demographic data was included in the survey instrument and was compared against their knowledge of cybersecurity concepts and subsequent scores.

I wanted to understand if age, gender, level of education, or how they rate their technical skills had any impact on the employee's ability to get a passing score on the post-test. This began with an ANOVA to obtain the descriptive statistic details for the collected demographics.

Table 8: Descriptive Statistics of Pre- and Post-Test Scores by Demographics

	Pre test score			Post test score		
	Mean	N	Std. Deviation	Mean	N	Std. Deviation
<b>Gender</b>						
Male	68.76	459	19.43	80.48	459	17.07
Female	67.92	556	19.29	83.09	556	15.44
Prefer not to answer	81.11	9	25.25	93.89	9	9.93
<b>Total</b>	<b>68.41</b>	<b>1024</b>	<b>19.43</b>	<b>82.02</b>	<b>1024</b>	<b>16.23</b>
<b>Age</b>						
18 to 25	67.29	65	16.69	80.85	65	15.55
26 to 35	68.57	254	19.47	83.62	254	15.91
36 to 45	70.05	302	20.30	82.27	302	16.43
46 to 55	67.12	267	18.22	79.53	267	15.78
56 and older	67.55	136	20.85	83.90	136	17.15
<b>Total</b>	<b>68.41</b>	<b>1024</b>	<b>19.43</b>	<b>82.02</b>	<b>1024</b>	<b>16.23</b>
<b>Highest Educational Degree held?</b>						
H.S. Diploma / GED	66.01	533	19.30	79.76	533	17.16
Associates	67.98	161	20.26	82.58	161	15.50
Bachelors	71.26	204	18.92	84.61	204	14.65
Masters	72.64	50	17.10	86.40	50	14.50
Doctorate	77.45	53	19.78	88.02	53	13.67
Not applicable	71.91	23	14.62	84.13	23	12.94
<b>Total</b>	<b>68.41</b>	<b>1024</b>	<b>19.43</b>	<b>82.02</b>	<b>1024</b>	<b>16.23</b>
<b>How would you rate your technical skills?</b>						
Basic knowledge	62.07	171	20.98	78.22	171	18.81
Limited experience	62.68	111	21.98	78.60	111	15.87
Intermediate knowledge	68.64	358	17.27	81.93	358	15.55
Advanced knowledge	72.61	303	18.13	85.03	303	15.07
Expert Knowledge	72.94	81	20.91	83.83	81	15.82
<b>Total</b>	<b>68.41</b>	<b>1024</b>	<b>19.43</b>	<b>82.02</b>	<b>1024</b>	<b>16.23</b>

The means reflect an improvement in the average mean score from the pre-test to the post-test based on the selected demographics.

To assess the third research question, a multivariate analysis was used to analyze the relationship between the demographic variables and the scores on the cybersecurity pre-test and post-test. It was determined that the variables related to how a person self-evaluates their technical skills were significantly related to the pre-test score ( $p=0.022$ ), but after taking the training, the post-test score was not significantly different suggesting that the training could have a short-period effect. The variable related to the subject's highest level of educational degree reached a very close significance at  $p=0.067$ .

Table 9: ANOVA results from variable intersections

Tests of Between-Subjects Effects						
Source	Dependent Variable	Type III Sum of Squares	df	Mean Square	F	Sig.
Corrected Model	Pre test score	95199.157 <sup>a</sup>	207	459.899	1.290	.008
	Post test score	63897.562 <sup>b</sup>	207	308.684	1.225	.029
Intercept	Pre test score	435803.119	1	435803.119	1222.109	<.001
	Post test score	610535.009	1	610535.009	2422.391	<.001
ED	Pre test score	3693.599	5	738.720	2.072	.067
	Post test score	1591.479	5	318.296	1.263	.278
AG	Pre test score	978.136	4	244.534	.686	.602
	Post test score	728.493	4	182.123	.723	.577
G	Pre test score	605.664	2	302.832	.849	.428
	Post test score	190.858	2	95.429	.379	.685
SE	Pre test score	4098.972	4	1024.743	2.874	.022
	Post test score	1711.719	4	427.930	1.698	.148
ED * AG	Pre test score	4846.082	18	269.227	.755	.754
	Post test score	2898.206	18	161.011	.639	.871
ED * G	Pre test score	354.409	5	70.882	.199	.963
	Post test score	875.235	5	175.047	.695	.628
ED * SE	Pre test score	2568.429	18	142.690	.400	.988
	Post test score	2909.649	18	161.647	.641	.868
AG * G	Pre test score	912.334	4	228.084	.640	.634
	Post test score	142.398	4	35.600	.141	.967
AG * SE	Pre test score	8543.071	16	533.942	1.497	.094
	Post test score	5546.626	16	346.664	1.375	.146
G * SE	Pre test score	4513.207	4	1128.302	3.164	.014
	Post test score	258.333	4	64.583	.256	.906
ED * AG * G	Pre test score	2200.895	18	122.272	.343	.995
	Post test score	2324.382	18	129.132	.512	.953
ED * AG * SE	Pre test score	17511.871	43	407.253	1.142	.249
	Post test score	9183.875	43	213.578	.847	.746
ED * G * SE	Pre test score	6677.146	14	476.939	1.337	.179
	Post test score	4193.441	14	299.531	1.188	.279
AG * G * SE	Pre test score	4037.290	15	269.153	.755	.729
	Post test score	3803.198	15	253.547	1.006	.446
ED * AG * G * SE	Pre test score	7853.199	26	302.046	.847	.686
	Post test score	7684.117	26	295.543	1.173	.253
Error	Pre test score	290984.933	816	356.599		
	Post test score	205663.155	816	252.038		
Total	Pre test score	5178726.000	1024			
	Post test score	7157725.000	1024			
Corrected Total	Pre test score	386184.090	1023			
	Post test score	269560.718	1023			

a. R Squared = .247 (Adjusted R Squared = .055)

b. R Squared = .237 (Adjusted R Squared = .043)

The intersection between gender and the self-skills assessment on the pre-test also resulted as significant ( $p=.014$ ). In most cases, female subjects rated their skills higher than their male counterparts suggesting some gender-wise differences in how these government employees self-assess their technical skills. This significant intersection may follow Anwar *et al.* (2017) and their suggestion that those differences based on gender “are statistically significant, gender-wise differences in terms of computer skills, prior experience, cues-to-action, security self-efficacy, and self-reported cybersecurity behavior” (p. 440).

A multiple regression analysis was further conducted on the pre-and post-test scores to examine the relationships between these variables and determine what are effective predictors. In both scoring instances, the variables for Education (ED) and technical skills (SE) were determined to be significant. Notably, gender (G) was additionally significant under the post-test analysis.



Table 10: Predictors will be kept in the stepwise model

Variables Entered/Removed <sup>a</sup>			
Model	Variables Entered	Variables Removed	Method
1	SE How would you rate your technical skills?		Stepwise (Criteria: Probability-of-F-to-enter <= .050, Probability-of-F-to-remove >= .100).
2	Ed What is your Highest Educational Degree held?		Stepwise (Criteria: Probability-of-F-to-enter <= .050, Probability-of-F-to-remove >= .100).

a. Dependent Variable: Pre test score

3	Gender Please state your gender.		Stepwise (Criteria: Probability-of-F-to-enter <= .050, Probability-of-F-to-remove >= .100).
---	----------------------------------	--	---

a. Dependent Variable: Post test score

A One-way ANOVA was used to determine the significant differences between the demographic variables and the post-test scores. The initial analysis was conducted against the age demographic and found that the mean difference was significant between the 26 to 35 group and the 46 to 55 group ( $p=.033$ ). The technical knowledge data was also observable as related to age or generation and how these government employees self-assess their technical skills based on their age. A steady increase and decline were notable as age increased. This could reflect a generational gap in technology usage and access based on the age difference between the two groups.

Table 11: ANOVA comparison between Age and Post-Test Scores

Multiple Comparisons						
Dependent Variable: Post test score						
Tukey HSD						
(I) Age Please select your age range	(J) Age Please select your age range	Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval	
					Lower Bound	Upper Bound
18 to 25	26 to 35	-2.77589	2.24864	.731	-8.9207	3.3689
	36 to 45	-1.42206	2.21193	.968	-7.4665	4.6224
	46 to 55	1.31432	2.23746	.977	-4.7999	7.4286
	56 and older	-3.05090	2.43933	.721	-9.7168	3.6150
26 to 35	18 to 25	2.77589	2.24864	.731	-3.3689	8.9207
	36 to 45	1.35384	1.37726	.863	-2.4098	5.1174
	46 to 55	4.09021*	1.41790	.033	.2156	7.9649
	56 and older	-.27501	1.71888	1.000	-4.9721	4.4221
36 to 45	18 to 25	1.42206	2.21193	.968	-4.6224	7.4665
	26 to 35	-1.35384	1.37726	.863	-5.1174	2.4098
	46 to 55	2.73638	1.35893	.260	-.9771	6.4499
	56 and older	-1.62885	1.67056	.866	-6.1939	2.9362
46 to 55	18 to 25	-1.31432	2.23746	.977	-7.4286	4.7999
	26 to 35	-4.09021*	1.41790	.033	-7.9649	-.2156
	36 to 45	-2.73638	1.35893	.260	-6.4499	.9771
	56 and older	-4.36522	1.70422	.078	-9.0223	.2918
56 and older	18 to 25	3.05090	2.43933	.721	-3.6150	9.7168
	26 to 35	.27501	1.71888	1.000	-4.4221	4.9721
	36 to 45	1.62885	1.67056	.866	-2.9362	6.1939
	46 to 55	4.36522	1.70422	.078	-.2918	9.0223

\*. The mean difference is significant at the 0.05 level.

The between-groups comparison reflects significance ( $p=.027$ ) making the model between age and post-test scores significant. The Age demographic factor has a significant effect on the post-test score, however, only between the specified age groups.

Table 12: ANOVA results post-test vs age.

ANOVA					
Post test score					
	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	2892.227	4	723.057	2.763	.027
Within Groups	266668.491	1019	261.696		
Total	269560.718	1023			

Another one-way ANOVA was used to evaluate the education level demographic and found two significant pair comparisons. It found that the post-test scores for users with

Bachelor's ( $p=.003$ ) and Doctorate ( $p=.005$ ) degrees were significantly higher when compared to those with only a high school diploma.

Table 13: Comparison between highest education level attained and post-test score.

Multiple Comparisons						
Dependent Variable: Post test score						
Tukey HSD						
(I) Ed What is your Highest Educational Degree held?	(J) Ed What is your Highest Educational Degree held?	Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval	
					Lower Bound	Upper Bound
H.S. Diploma / GED	Associates	-2.82154	1.44393	.370	-6.9442	1.3011
	Bachelors	-4.85175 <sup>*</sup>	1.32190	.003	-8.6260	-1.0775
	Masters	-6.64390	2.37482	.059	-13.4244	.1366
	Doctorate	-8.26277 <sup>*</sup>	2.31255	.005	-14.8655	-1.6601
	Not applicable	-4.37434	3.41943	.796	-14.1373	5.3887

The descriptive statistics reflect a gradual increase in the mean of the post-test score as the highest level of education attained increases.

Table 14: Descriptive statistics Education vs. Post-test scores

Descriptives								
Post test score								
	N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Minimum	Maximum
					Lower Bound	Upper Bound		
H.S. Diploma / GED	533	79.7561	17.16343	.74343	78.2957	81.2165	.00	100.00
Associates	161	82.5776	15.50308	1.22181	80.1647	84.9906	20.00	100.00
Bachelors	204	84.6078	14.65004	1.02571	82.5854	86.6303	30.00	100.00
Masters	50	86.4000	14.49982	2.05058	82.2792	90.5208	50.00	100.00
Doctorate	53	88.0189	13.66986	1.87770	84.2510	91.7867	40.00	100.00
Not applicable	23	84.1304	12.93798	2.69776	78.5356	89.7252	65.00	100.00
Total	1024	82.0166	16.23269	.50727	81.0212	83.0120	.00	100.00

This allows the inference that higher levels of education can improve the subject's ability to successfully answer questions on the cybersecurity knowledge quiz.

Table 15: ANOVA results in posttest vs Highest Education Level Attained.

ANOVA					
Post test score	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	7116.928	5	1423.386	5.521	<.001
Within Groups	262443.789	1018	257.803		
Total	269560.718	1023			

The ANOVA results for the highest level of education attained are significant ( $p < .001$ ) and we can infer that the educational degrees affect the subject's ability to answer questions correctly on the cybersecurity knowledge test after the training course has been administered.

Table 16: Post Hoc Test Comparison of Gender

Multiple Comparisons						
Dependent Variable: Post test score						
Tukey HSD						
(I) Gender Please state your gender.	(J) Gender Please state your gender.	Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval	
					Lower Bound	Upper Bound
Male	Female	-2.61422*	1.01900	.028	-5.0060	-.2225
	Prefer not to answer	-13.40959*	5.43854	.037	-26.1745	-.6446
Female	Male	2.61422*	1.01900	.028	.2225	5.0060
	Prefer not to answer	-10.79536	5.42941	.116	-23.5389	1.9482
Prefer not to answer	Male	13.40959*	5.43854	.037	.6446	26.1745
	Female	10.79536	5.42941	.116	-1.9482	23.5389

\*. The mean difference is significant at the 0.05 level.

A separate analysis found that gender also significantly affected the scores on the post-test. The comparison between males and females was significant with a p-value of .028 and the between-groups analysis was significant at  $p=.003$ .

Table 17: ANOVA results posttest vs Gender

<b>ANOVA</b>					
Post test score					
	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	2998.139	2	1499.069	5.742	.003
Within Groups	266562.579	1021	261.080		
Total	269560.718	1023			

An analysis of the means for the post-test scores shows that female participants scored slightly higher than their male counterparts. This is in agreement with the suggestion by Anwar *et al.* (2017) that the ability to perceive and accept risk varies by gender and females are generally more concerned with perceived risk as opposed to their male counterparts. Which may explain why women scored slightly higher than male subjects. However, Anwar *et al.* (2017) also suggested that male subjects “place a greater influence on attitude toward using technology than women” (p. 440).

Table 18: Analysis of Means for Gender

<b>Post test score</b>			
Tukey HSD <sup>a,b</sup>			
Gender Please state your gender.	N	Subset for alpha = 0.05	
		1	2
Male	459	80.4793	
Female	556	83.0935	

The final ANOVA was used to understand the significance of self-assessed technical skills against the subject’s post-test score. The comparison between Basic and Advanced technical knowledge was found to be significant ( $p < .001$ ) as was the comparison between Limited and Advanced technical knowledge ( $p = .003$ ).

Table 19: Pairwise comparison between self-assessed technical skills

Multiple Comparisons						
Dependent Variable: Post test score						
Tukey HSD						
(I) SE How would you rate your technical skills?	(J) SE How would you rate your technical skills?	Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval	
					Lower Bound	Upper Bound
Basic knowledge - You have a common knowledge or an understanding of basic computer concepts.	Limited experience - You have experience gained experience on-the-job. You are expected to need help when performing tec	-.38723	1.95735	1.000	-5.7360	4.9616
	Intermediate knowledge - You are able to successfully complete computer tasks as requested.	-3.71100	1.49277	.095	-7.7902	.3682
	Advanced knowledge - You can perform work on your computer without assistance.	-6.81663 <sup>*</sup>	1.53594	<.001	-11.0138	-2.6194
	Expert Knowledge - You are known as an expert in this area. You can provide guidance to co-workers.	-5.61079	2.16602	.073	-11.5298	.3082
Limited experience - You have experience gained experience on-the-job. You are expected to need help when performing tec	Basic knowledge - You have a common knowledge or an understanding of basic computer concepts.	.38723	1.95735	1.000	-4.9616	5.7360
	Intermediate knowledge - You are able to successfully complete computer tasks as requested.	-3.32377	1.74456	.315	-8.0911	1.4435
	Advanced knowledge - You can perform work on your computer without assistance.	-6.42940 <sup>*</sup>	1.78164	.003	-11.2980	-1.5608
	Expert Knowledge - You are known as an expert in this area. You can provide guidance to co-workers.	-5.22356	2.34666	.171	-11.6362	1.1891

An evaluation of the Mean of the post-test scores and the self-assessed technical skills provides a better assessment of how the participants rate their technical skills and how that affects their scores on the cybersecurity knowledge survey.

Table 20: ANOVA results posttest vs Self-Assessed Skill Level

<b>ANOVA</b>					
Post test score					
	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	6787.803	4	1696.951	6.581	<.001
Within Groups	262772.915	1019	257.873		
Total	269560.718	1023			

A steady increase in the Mean score is observable as the level of technical knowledge increases in the resulting descriptives table.

Table 21: Descriptive Statistics for Self-Assessed Technical Skills and Post-test Scores

<b>Descriptives</b>								
Post test score								
	N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Minimum	Maximum
					Lower Bound	Upper Bound		
Basic knowledge - You have a common knowledge or an understanding of basic computer concepts.	171	78.2164	18.80723	1.43822	75.3773	81.0555	20.00	100.00
Limited experience - You have experience gained experience on-the-job. You are expected to need help when performing tec	111	78.6036	15.87123	1.50643	75.6182	81.5890	40.00	100.00
Intermediate knowledge - You are able to successfully complete computer tasks as requested.	358	81.9274	15.55420	.82206	80.3107	83.5441	20.00	100.00
Advanced knowledge - You can perform work on your computer without assistance.	303	85.0330	15.06604	.86552	83.3298	86.7362	.00	100.00
Expert Knowledge - You are known as an expert in this area. You can provide guidance to co-workers.	81	83.8272	15.81676	1.75742	80.3298	87.3245	35.00	100.00
Total	1024	82.0166	16.23269	.50727	81.0212	83.0120	.00	100.00

The effect of certain demographic variables on the scores for the cybersecurity knowledge test at the post-test level was determined to be significant. The analysis has determined that the demographic variables for gender ( $p=.003$ ) and age ( $p=.027$ ) have a

significant effect on post-test scores. The demographic variables for the highest level of education attained ( $p < .001$ ) and the subject's self-assessed technical skills ( $p < .001$ ) have a stronger effect on the subject's ability to correctly answer questions on the cybersecurity knowledge test.

The cybersecurity knowledge quiz tests an internet user's understanding of cybersecurity issues and concepts. A user's ability to identify and report a suspected cyber-attack attempt (phishing) allows the organization's security teams to take further actions to contain and prevent further incursion or compromise of the organization. The questions asked in the cybersecurity knowledge quiz measured whether the participants could effectively identify specific cybersecurity concepts that could lead to a compromise of the organization. The following will compare the success rate of Cameron County employees against the results of the original study by Kenneth Olmstead and Aaron Smith for Pew Research in 2017.

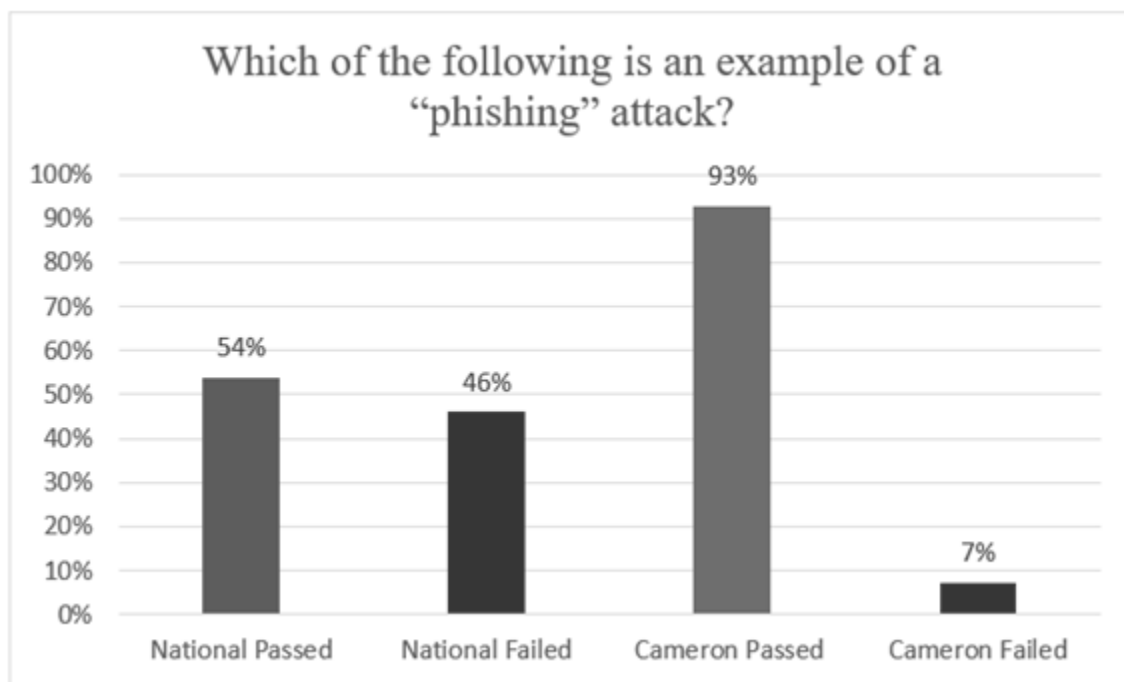


Figure 11: Identifying Phishing Techniques



The majority of the participants (93%, n =1024) were able to successfully identify that all the possible responses were different tactics used to effectively “phish” users. The remaining 65 users (6%) answered incorrectly and less than 1% were unsure. This is compared to the national 2016 Pew research study by Olmstead and Smith which found that 54% of those studied correctly identified and the remaining 46% were incorrect or unsure.

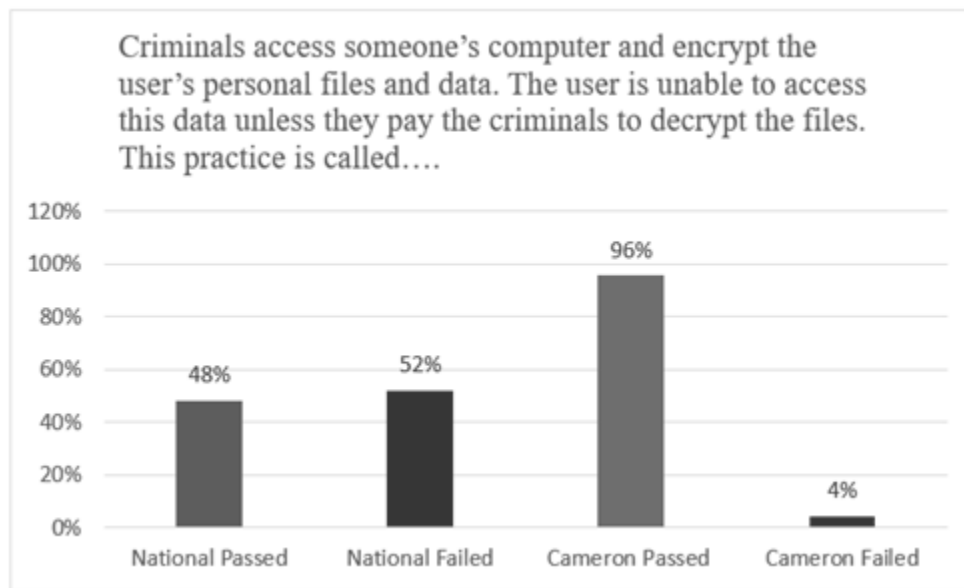


Figure 12: What is ransomware?

The majority of the participants (96%, n =1024) of the 1200 Cameron County employees were able to successfully define the threat known as ransomware, a method used by cyber criminals to monetize their actions. Ransomware is often the subsequent result of a phishing attack. The remaining 45 users (4%) answered incorrectly or were unsure. The national Pew survey found that 48% of the participants studied selected ransomware, while 52% were incorrect or unsure.

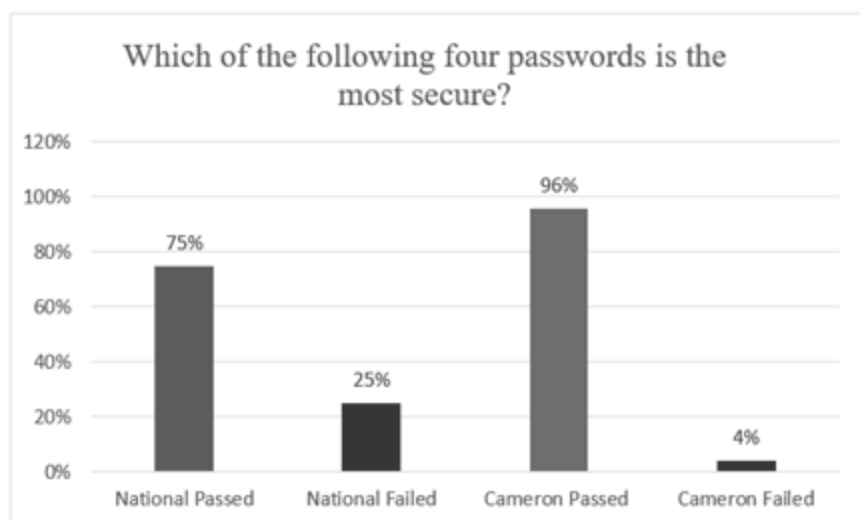


Figure 13: Secure Passwords

Secure passwords are a best practice against cyber-attacks and again 96% (n =1024) of the 1200 Cameron County participants were able to successfully identify a properly formed and more security-minded password, whereas only 4% were not able to do so. The national Pew survey found that 75% of the participants studied selected the secure password, while the remaining 25% were incorrect or unsure.

Knowledge of cybersecurity concepts can lead to improved cybersecurity habits and can have a risk-reducing impact on an organization's cybersecurity posture. The results of the cybersecurity knowledge quiz presented to the participants in Cameron County and adapted from a 2016 survey conducted by Pew Research reflected that Cameron County employees well exceeded the averages found by the national survey. An employee's ability to mitigate a cyber threat can be based on their ability to identify that threat and report it to the organization's security department. Preventing a breach of the "human firewall" reduces the probability of an organizational breach and employees being able to identify and report suspicious activity allows

the organization to take appropriate action, all of which lead to an improved security posture (Diaz *et al.*, 2020; Chowdhury *et al.*, 2019).

### **Summary**

This study examined the effect of a cybersecurity training course on government employees. It looked at their ability to mitigate threats in their limited capacity and whether any demographical factors improved these outcomes. The study consisted of reviewing archival data from four years (2018-2022) and measured with a pre and post-test included in a survey presented to all employees in 2021. Success was measured in an employee's ability to identify and report cybersecurity incidents in the form of phishing attempts. This chapter presented the results obtained from the analyses used to test the hypotheses outlined in this study. The next chapter, Chapter Five, presents the conclusions, interpretations, and implications suggested by those results.

## CHAPTER V

### CONCLUSIONS, INTERPRETATIONS, AND IMPLICATIONS

#### **Introduction**

This chapter presents the conclusions, interpretations, and implications related to the core findings of this study. Future research directions will also be discussed. The purpose of this study is to analyze the effect of a cybersecurity awareness training program on government employees' knowledge of cybersecurity issues and their ability to mitigate cybersecurity threats. To achieve this purpose, the following research questions were developed and tested and the results were presented in the prior chapter.

- What is the effect of a cybersecurity awareness training program on government employees' knowledge of cybersecurity issues and practices?
- What is the effect of a cybersecurity awareness training program on government employees' ability to mitigate cybersecurity threats?
- What demographic factors are related to government employees' knowledge of cybersecurity issues and practices and their ability to mitigate cybersecurity threats?

The study tested the employees of the Cameron County government during their annual cybersecurity training response to Texas House Bill 3834. The research hypothesized that cybersecurity training had a positively related to the knowledge and mitigation ability of

government employees. He *et al.* (2020) argue “the best cybersecurity investment an organization can make is better training” (p. 204).

The purpose of this study is to analyze the effect of a cybersecurity awareness training program on government employees’ knowledge of cybersecurity issues and their ability to mitigate cybersecurity threats. Their ability to help mitigate a potential compromise can make them part of the organization's security solution as opposed to being the primary attack vector for a cyber attacker (Costa *et al.*, 2019). An employee base that can work at alerting their organization to an attempted compromise puts that organization in better standing with its security posture.

### **Conclusion and Interpretation for Hypothesis One**

To test the first research hypothesis, there is a statistically significant positive effect of a cybersecurity awareness training program on government employees’ knowledge of cybersecurity issues and practices as measured by a comparison of their pre-and post-test scores, a repeated measures ANOVA was used. Table 3 on page 78, presents the results, which show a significant increase in the mean scores between pretests and posttests. The test scores improved by 13.61% between the pre-test and post-test. Therefore, the research hypothesis was accepted. There was a statistically significant positive effect of a cybersecurity awareness training program on government employees’ knowledge of cybersecurity issues and practices as measured by a comparison of their pre-and post-test scores.

This finding is supported by Oancea *et al.* (2019) who found that “most cyber-attacks exploit the vulnerability of users and only some of them exploit the technical flaw” and the only remedy to that vulnerability is to improve the security-based situational awareness of their

workforce (p. 46). Based on pre-and post-test scores, employees who participated in the mandatory cybersecurity awareness training benefitted from and increased their knowledge of cybersecurity issues and practices. Accordingly, Kortjan and Solms (2014) suggest that management security initiatives and enhanced security tools are successful when used in conjunction with cybersecurity training to strengthen cybersecurity safety and reduce threats. Daengsi *et al.* (2021) further that “the risks from this kind of threats can be reduced if the employees have cybersecurity awareness” (p. 102). In summary, while improved cybersecurity awareness as a result of training in and of itself cannot mitigate cybersecurity threats, when combined with other organizational efforts it can help to reduce threats caused by the human factor.

### **Conclusion and Interpretation for Hypothesis Two**

To test the second research hypothesis, there is a statistically significant positive effect of a cybersecurity awareness training program on government employees’ ability to mitigate cybersecurity threats as measured by the frequency of mitigated cybersecurity threats identified before and after the training, mock phishing attempts for the previous five years were collected and compared. The first mock-phishing attempt conducted in the Fall of 2018 reflected that the employees of Cameron County local government (N=1180) were found to be highly susceptible (70.2%) to common phishing techniques as reflected in the results Table 4 on page 80. This was followed by a survey conducted in September 2019 that further reflected that a sample of this population felt that they were vulnerable (55.31%) to cybersecurity attacks as reflected in the table below.

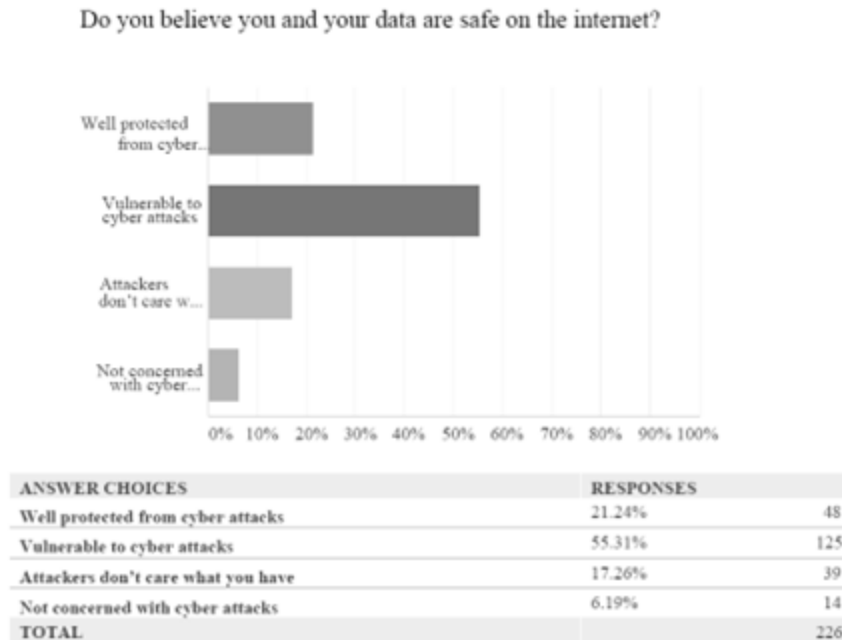


Figure 14: 2019 Survey question result.

After the initial H.B. 3834 mandated training course was provided in May 2019, A phishing campaign was conducted in October. The results of that mock phishing campaign (N=1298) reflected a significant improvement from the year before, lowering the susceptibility to 19.4%. Mandated training continued in the Spring and the observance of National Cybersecurity Awareness Month (NCSAM) in the Fall provided a continuous focus on cybersecurity. These focusing events offered additional enforcement in the form of mock phishing campaigns which continued to lower the reflected susceptibility of the studied population. Off-cycle phishing campaigns in the Spring and Summer of 2022 were conducted on smaller samples of the population and saw fewer employees being compromised and more employees reporting the phishing e-mail to Cameron County's Information Technology Department effectively aiding in the mitigation of a cybersecurity compromise attempt.

These findings suggest that there was a statistically significant positive effect of a cybersecurity awareness training program on government employees' ability to mitigate cybersecurity threats as measured by the frequency of mitigated cybersecurity threats identified before and after the training. The cybersecurity program in Cameron County started in 2018 and expanded with the mandating of cybersecurity training in 2019, and as of the Summer of 2022. Based on the results of mock phishing attempts, where employees were sent simulated e-mails attempting to compromise employees in a controlled manner, reflected a significant statistical decrease in the projected susceptibility of its employees. The lowered susceptibility suggests that there is a lowered likelihood that an employee would be compromised by phishing e-mail. The findings also reflected an increase in the target group's ability and willingness to mitigate these mock phishing attempts by reporting them to Cameron County's security team. As with the first research hypothesis, there was a notable drop in progress which can also be attributed to limited cybersecurity training efforts possible as a result of the COVID-19 pandemic and employees working remotely. This was made evident by the comparison of the full population susceptibility results of 2019 (19.4%) and 2022 (30.33%), which continues to suggest that cybersecurity education needs to be consistent to remain effective.

Zwilling *et al.* (2020) categorized levels of cybersecurity awareness as low, medium, and high; which established how neglectful or attentive an internet user is toward the proper usage of technology and knowledge of cyber threats. That awareness score functions similarly to the level of susceptibility established by mock phishing tests conducted by Cameron County's security team, the lower the susceptibility the higher the organization's security posture. This collected data assists the organization's security team in understanding the level of awareness in the organization and knowing when to take corrective action. Tirumala *et al.* (2019) also



suggested that collecting metrics to understand the existing knowledge “provides a comprehensive understanding of the cybersecurity awareness” of a given population (p. 1). In Summary, these findings suggest that using phishing exercises and measuring an organization’s cybersecurity awareness allows management to understand what their workforce knows and if additional training or education is needed to improve their cybersecurity awareness.

### **Conclusion and Interpretation for Hypothesis Three**

To test the third research hypothesis, there is a statistically significant relationship between employees’ cybersecurity awareness scores and demographic variables such as gender, age, self-assessed technical skills, and their highest level of education attained, an ANOVA was used against the results of the survey instrument which included the Cybersecurity Knowledge Quiz. The Pew research study by Olmstead and Smith (2017) showed some modest significance between age and cybersecurity knowledge. As Daengsi *et al.* (2021) and Diaz *et al.* (2020) argued cybersecurity awareness is impacted by several demographic factors, including, educational background, work experience, the field of study, gender, age, and socioeconomic status.

The descriptive statistics on Table 8 on page 86 present the results of the ANOVA that was conducted on the population’s post-test score and whether the employee achieved a passing grade (60 or better), these were compared against the following demographic variables:

- Gender (G)
- Age Range (AG)
- Highest Education Level attained (ED)
- How do they rate their technical skills (SE)

The significance threshold was set at .05 and the correlation is significant at the 0.01 level (2-tailed). The results of the analysis found that the post-test analysis that the highest level of education attained ( $p < .001$ ,  $r = .152$ ), and the skills self-assessment ( $p < .001$ ,  $r = .147$ ) were consistently and highly significant. Whereas gender ( $p = .003$ ,  $r = .095$ ), and age ( $p = .027$ ,  $r = -.022$ ) were only significant at the post-test level and not during the pre-test.

Fatokun *et al.* (2019) suggested that these demographic factors can be used to enhance the effectiveness and perhaps even better target cybersecurity awareness curriculum. These findings suggest that an employee's level of education and how they rate their technical knowledge reflected a statistically significant positive effect when concerning the results of the cybersecurity awareness training. Dawson and Thomson (2018) argued: "that the people who operate within the cyber domain need a combination of technical skills, domain-specific knowledge, and social intelligence" for successful cyber performance (p. 1). These same results found that there was no consistent effect that was statistically significant brought by the demographic variables of gender or age. Therefore, higher levels of academic education and technical skill do support the acceptance of the hypothesis.

### **Implications for Research**

The threat of cyberattacks against government agencies is serious enough that the requirement for training was mandated by the State of Texas. The Texas House of Representatives passed House Bill 3834 in 2019 as a result of the increase in cyberattacks on government agencies, it was later amended with house bill 1118 in 2021 which makes non-compliant agencies ineligible for State grant funding (Yazdanpanahi, 2021). Government agencies need to educate their employees on cybersecurity concepts and ensure that they can

effectively identify phishing attempts and alert their organization's cybersecurity team to take further action.

Training a workforce is not an easy process as Kessler and Ramsay (2013) argued that it is difficult “to provide technical literacy for” a population of employees on what may be considered highly technical content that they didn’t know they needed (p. 41). This study was used to determine the effect that a cybersecurity awareness training program had on government employees’ knowledge of cybersecurity issues and their ability to mitigate cybersecurity threats. The training program provided knowledge of cybersecurity concepts and a pre-test and post-test were used to assess the population’s knowledge and understanding of those concepts sufficiently to apply them. “Education plays a critical part” in an organization's efforts “in cultivating a culture of secure behavior” (Kortjan and Solms, 2014, p. 29). The results of this study suggest that taking cybersecurity training is effective over time in reducing an employee’s susceptibility to cybersecurity compromise. However, the results of the study also reflect that the effect can be short-lived and that this government agency (as well as others) should continually enforce cybersecurity training and include random phishing tests to maintain the effect. This is consistent with the recommendation that cybersecurity not only needs to be relevant but also consistently provided (Kortjan and Solms, 2014; de Bruijn and Janssen, 2017; Adorjan and Ricciardelli, 2019; Yazdanpanahi, 2021). Therefore, regular and consistent cybersecurity education and training are effective tools for helping employees identify and potentially help mitigate cybersecurity threats.

The pre-test and post-test consisted of a cybersecurity knowledge survey adapted from Pew Research’s Cybersecurity Knowledge Quiz (Smith, 2017). The target group (N = 1024) of Cameron County government employees took the Cybersecurity Knowledge. The results of this

study suggest that the employee's knowledge of specific cybersecurity concepts improved from the pre-test to post in their awareness of specific cybersecurity concepts.

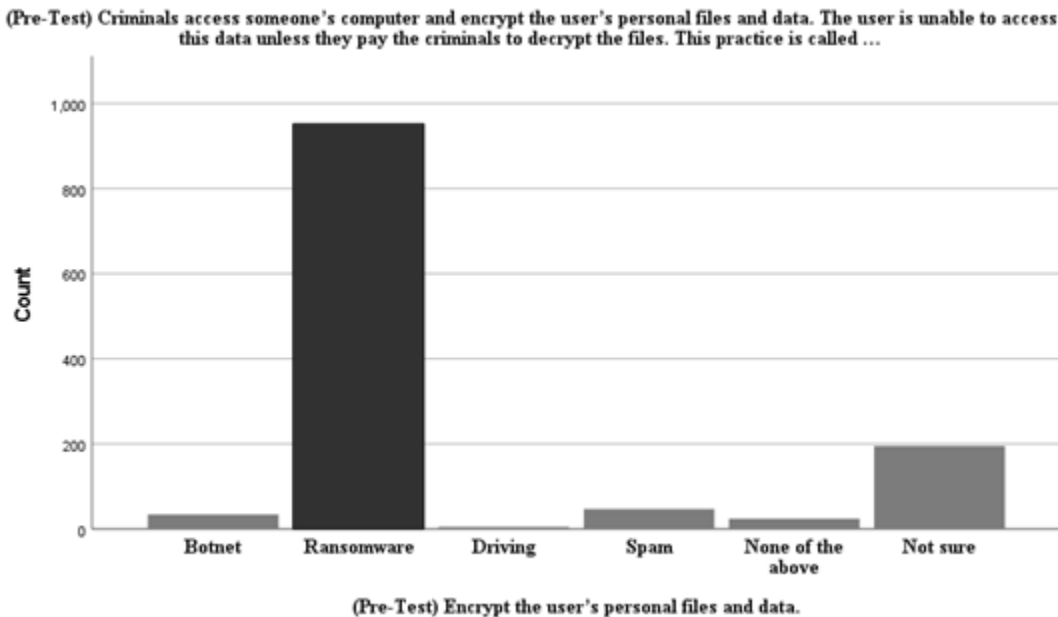


Figure 15: Pre-test results for ransomware

Research has shown that ransomware-related cyberattacks are on the rise and targeting employees with tactics including social engineering and phishing, attacks which often come at a higher cost (Kweon *et al.*, 2019; Yazdanpanahi, 2021; Kostyuk and Wayne, 2020). The results for question #15, which asks if the employee knows what ransomware is, show that many employees were able to answer correctly before partaking in the training (pre-existing knowledge) and an increase was reflected for additional employees after the training. The results suggest employees' knowledge and awareness about Ransomware increased from 84% to 95% after the training.

**Criminals access someone's computer and encrypt the user's personal files and data. The user is unable to access this data unless they pay the criminals to decrypt the files. This practice is called ... ?**

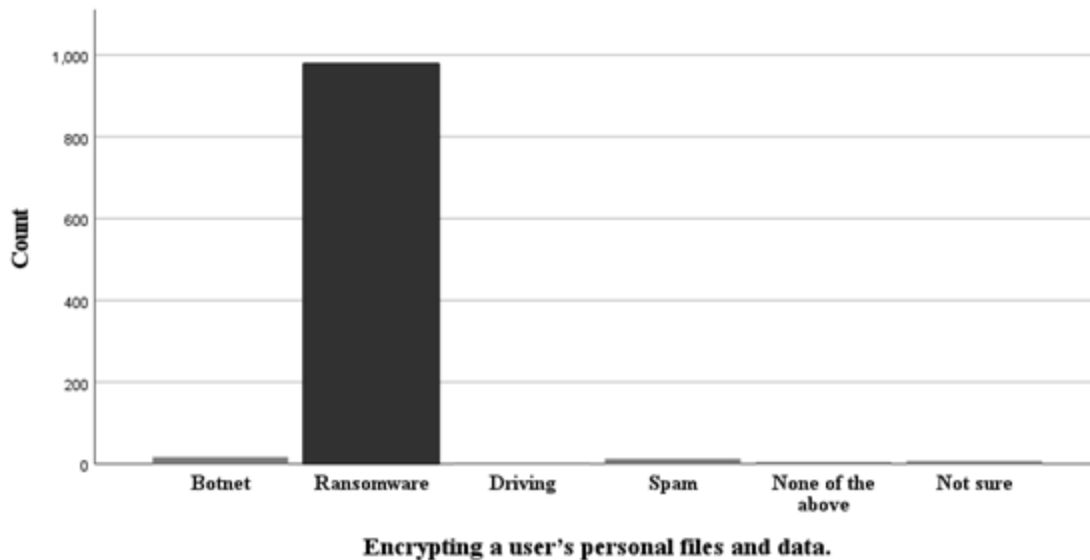


Figure 16: Post-test results for ransomware

This is also reflected in the lowering click rate on Figure 9 page 84 and the lowered phishing-prone levels reflected by the annual phishing campaigns. When employees have a better understanding of what ransomware is and how an organization can be compromised by a phishing e-mail, can aid in the mitigation process.

Although the results of this study supports the need for cybersecurity training amidst the growing threat of ransomware attacks against organizations both public and private, this study suggests that cybersecurity training has a positive effect on making government employees more aware of cyber threats. However, this study can not provide a sufficient prediction of the future actions of one of these employees when placed in a cybersecurity compromise situation. To a certain extent, the results of the study identified that a significant portion of the target group understood the training content sufficiently enough to lower the overall susceptibility of the organization. The Cybersecurity Knowledge Quiz and the phishing tests help identify those

groups that scored low or were successfully phished and allow them to be monitored more closely and further trained. This will require additional changes to the cybersecurity program at Cameron County, including training, best practices, and methods of testing. These changes to practice are discussed in the next section as recommended areas for improvement for the security program in Cameron County.

### **Implications for Practice**

The results of this study suggest a positive impact on cybersecurity awareness of the target population, however, the Mean post-test score was 82.02%, and the Grand Mean of 75.21%. This suggests the target population is passing the quiz, but not with a 100%. This compounded with the results reflecting that there are still employees that were not able to identify what ransomware is (5% of the target group) should be concerning for the organization. The fact that it only takes a mistake from a single employee to trigger a major cybersecurity threat, can put the organization where the needs of its constituents can go met (Axelrod, 2019). Addressing these potential deficiencies will require changes to current best practices and training procedures. The suggested changes should be targeted not only at the specific users that are having difficulty with the content but also focusing on the topics in which they are deficient, all the while attempting to maintain the status quo of the entire organization's cybersecurity awareness and posture.

Bruijn and Janssen (2017) argue that “limited visibility, socio-technological complexity, ambiguous impact, and the contested nature of fighting cybersecurity complicates” the ability to not only defend but effectively train against rapidly changing threat vectors (p.2). Phishing attempts often attempt to collect user credentials to be used in an attack at a later time (Daengsi *et al.*, 2021; Yazdanpanahi, 2021). The Cybersecurity Knowledge Quiz asked questions

regarding complex passwords and additional methods for secure authentication. In addition to additional training, government employees should be able to develop strong passwords that are not easily guessed or shared with co-workers. Question 16 of the Cybersecurity Knowledge Quiz asked the target group to identify the strongest password in the provided list. Tirumala *et al.* (2019) found it “alarming to see that 68% are using common passwords across various authorizations and only about 30% of users are having strong passwords with at least a number, an alphabet, and a special character” (p. 4). The results of the study indicated that at least the target population was able to identify a strong password and exceeded the results of the national study conducted by Pew Research.

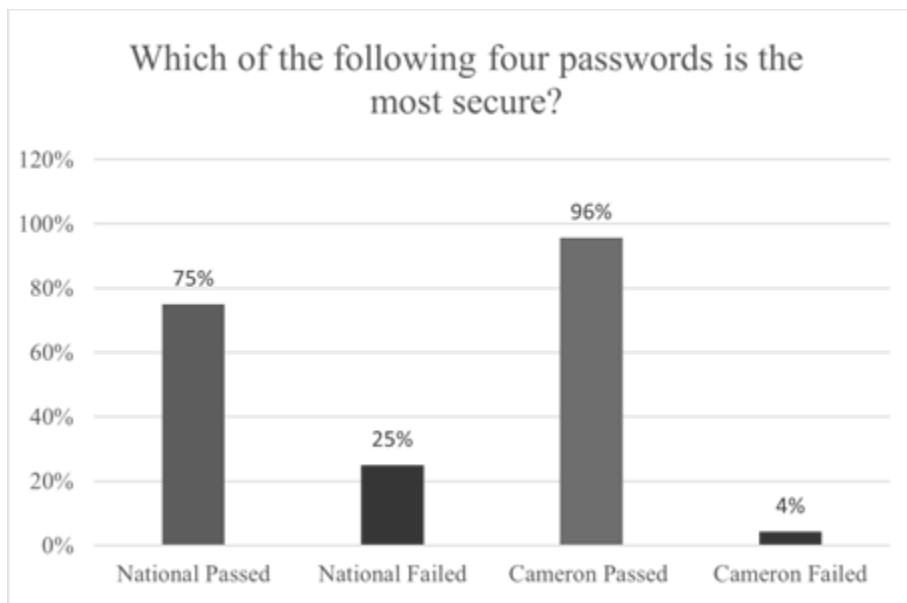


Figure 17: Strong Passwords National vs. Cameron County

Tirumala *et al.*, (2019) further found that when most computers users are “asked to create a password, the majority of the people tend to follow minimum requirements that are mandated by the software, website, or social media platform rather than thinking about how secure their

password is” (p. 3). This is reflected in the results that suggest that there is still a small group (4%) that still are unable to identify or possibly create a strong password.

However, even strong passwords can still be compromised by a phishing attack if an employee does not have proper cybersecurity awareness. Walsh (2020) argues that “passwords alone are not secure because weak passwords are easily hacked by using a list of common passwords, and complex passwords can be deciphered due to human predictability” (p. 1). The research suggests that passwords are more secure when combined with a second level of authentication, which is also known as multi-factor authentication (Matthews, 2012; Walsh, 2020; Weber *et al.*, 2008). Multi-Factor Authentication is the act of using a secondary authentication method in combination with a password to verify your identity, this includes but is not limited to a pin code, security questions, or a biometric interface (i.e. fingerprint) (CISA, 2020). Question 15 of the Cybersecurity Knowledge Quiz asked the target group to identify an example of multi-factor authentication. Tirumala *et al.*, 2019 found it “surprising to see that about 45% of participants are familiar with two-factor authentication” (p. 4). The results of the study indicated that only 67% of the target population was able to identify the proper example, which was still better than the 10% from the national study.



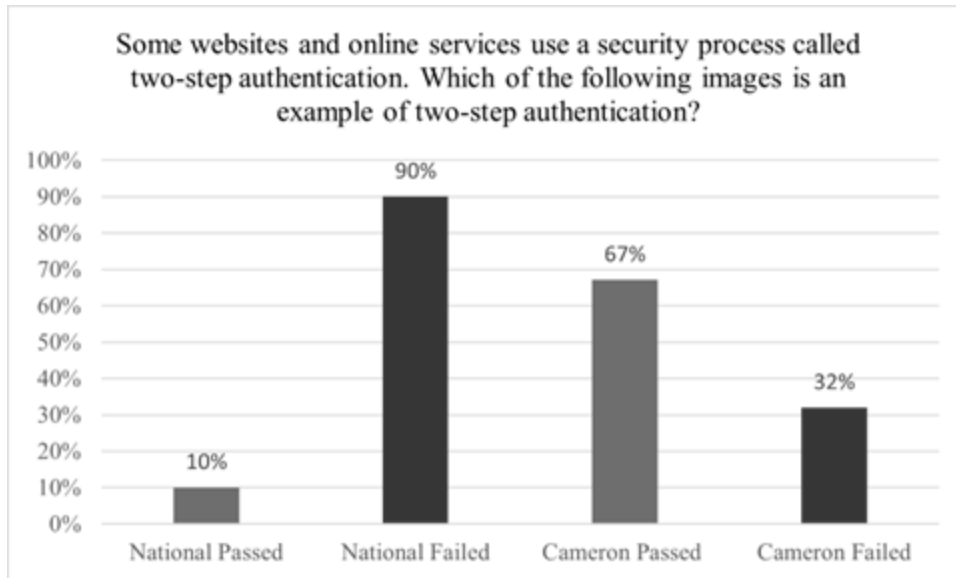


Figure 18: MFA identification National vs. Cameron County

The results suggest that there is still further training required regarding the effective use of two-factor authentication. Passwords, even strong passwords lose their effectiveness in a phishing attack, especially when employees lack basic cybersecurity awareness. Cybersecurity training needs to be frequently updated and consistently provided and paired with safer internet practices that include but are not limited to these additional authentication practices (Kortjan and Solms, 2014; de Bruijn and Janssen, 2017; Adorjan and Ricciardelli, 2019; Yazdanpanahi, 2021).

A strong password consists of multiple characters in upper-case/lower-case, numbers 0-9, and special characters (#%@...) and be changed at regular intervals to make them more difficult to guess or force (Habib *et al.*, 2018). Matthews (2012) suggests that passwords are simply not enough and that a secondary authentication method should be added to secure a user's identity. These authentication methods known as 'factors' can be defined as "something you know" such as a pin code, "something you have" such as an authenticator app on a mobile phone, or

“something you are” such as a fingerprint or retinal scan (biometric) (CISA, 2020; Walsh, 2020; Matthews, 2012).

### **Recommendations for Future Research**

This study examined the effect that cybersecurity training had on government employees' knowledge of cybersecurity concepts and their ability to aid in the mitigation process. Due to cybersecurity's critical entanglement with the continued operations of most organizations and specifically government agencies, success in cybersecurity education is important. Research has demonstrated that the employee or “human firewall” is often the first attack vector in an organized cybersecurity attack, they are often the easiest way into an organization (Diaz *et al.*, 2020; Chowdhury *et al.*, 2019). Kemper (2019) further suggests that “employees pose the greatest cybersecurity threats” to their corporate data and networks, especially when they are not trained to be cybersecurity aware (p. 11).

For this reason, all organizations, especially government agencies need to ensure that cybersecurity training and education are a priority. A cybersecurity compromise of a public organization, like a government agency can affect its ability to operate and for a government agency, it hinders its ability to provide services to the public (Axelrod, 2019; Yazdanpanahi, 2021). The ability of employees to understand cybersecurity concepts and identify phishing e-mails is critical because often cases the employee will see them before the Information Technology and Security department, making them the first line of defense. Based on the findings in this study, the following recommendations are for future studies.

1. Research addressing the efficacy of cybersecurity training for long-term knowledge retention. Understanding that cybersecurity training could have a short-period effect

warrants future studies to understand if increasing the amount of training or increasing the frequency maintains or improves the level of susceptibility to phishing for the organization.

2. Research considering the effect of other demographic variables on cybersecurity awareness and behaviors. These variables can include but not be limited to professional capacity, socioeconomic status, and level of government. These additional demographics may provide further information on how government employees are impacted by cybersecurity training.
3. Research that more closely considers the effect of gender on cybersecurity awareness and behaviors. Fatokun *et al.* (2019) suggested that gender played a role in technical assessments and the results of this study found that the intersection between technical skills and gender was highly significant during the pre-test but did not carry over to the post-test, further investigation of the relationship between these variables should be conducted.
4. Research addressing the efficacy of cybersecurity training on other business sectors, including but not limited to the education and private sectors of business that are just as susceptible to cyberattacks and the effects of the attack are likely to be felt outside the organization.
5. Research addressing the efficiency of cybersecurity training relating to the compromising effects of social engineering or other methods of security compromise. This study primarily focused on the use of the e-mailed phishing variety. Social engineering or a threat actor utilizing context clues from social media to gain a sense of trust from a target and eventually compromising access to an organization is another serious attack vector.

Medlin, B., Cazier, J., and Foulk, D (2008) argue that social engineering is a serious threat to keeping information secure and increases “increased opportunities for exploitation that exist in today's digital world” (p. 72). Therefore, this additional method requires further study and the effects of training, and the types of training needed to combat social engineering.

### **Summary**

Government agencies must protect themselves against cybersecurity attacks, and while investment in effective security solutions adds a layer of protection, they should be used in conjunction with cybersecurity awareness training. Diaz, *et al.* (2020) and Chowdhury, *et al.* (2019) agree with other cybersecurity professionals that the human factor is consistently going to be breached. Government agencies will continue to be targets of cybersecurity attacks due to the amount of sensitive data they collect, and their employees will continue to be a primary attack vector. While technology tools can be effective in combating an active cyber compromise, the human factor or the organization's employees are the first to see the phishing attempt before the compromise occurs. Several research and security experts suggest that one way to mitigate a cybersecurity attack is through education in the form of regular cybersecurity training (Costa *et al.*, 2019; Heartfield and Loukas, 2018; Kortjan and Solms, 2014; CISA, 2020). Miller (2017) agrees that “there is still much work to be done on the security awareness training front” (p. 1). The underlying goal is to better inform and prepare the studied population for real-world cybersecurity scenarios. The cost of a cybersecurity compromise significantly increases as the demand for e-government and public information access via the Internet increases (MacManus *et al.*, 2013; Yazdanpanahi, 2021). A systematic approach to cybersecurity defenses combined with a regularly trained cybersecurity-aware employee base can improve a government agency's

resilience against cyber threats. This could translate into a lasting change in attitudes, understanding, and behavior regarding their personal and professional awareness of cybersecurity concepts.

## REFERENCES

- Adorjan, M., and Ricciardelli, R. (2019). Student perspectives towards school responses to cyber-risk and safety: The presumption of the prudent digital citizen. *Learning, Media and Technology*, 44(4), 430-442. Retrieved from <http://search.ebscohost.com.ezhost.utrgv.edu:2048/login.aspx?direct=true&db=a9handAN=139257679&site=ehost-live>
- Anwar, M., He, W., Ash, I., Yuan, X., Li, L., and Xu, L. (2017). Gender difference and employees' cybersecurity behaviors. *Computers in Human Behavior*, 69, 437-443.
- Axelrod, J. (2019). The right playbook to fight against ransomware. American City and County Exclusive Insight, N.PAG. Retrieved from <http://search.ebscohost.com.ezhost.utrgv.edu:2048/login.aspx?direct=true&db=a9handAN=140085417&site=ehost-live>
- Baier, A. C. (1970). Act and intent. *The Journal of Philosophy*, 67(19), 648-658.
- Black, L., Scala, N. M., Goethals, P. L., and Howard, J. (2018). Values and trends in cybersecurity. In Proceedings of the Institute of Industrial and Systems Engineering Conference. 1820-1825. Orlando, FL: Institute of Industrial and Systems Engineers.
- de Bruijn, H., and Janssen, M. (2017). Building cybersecurity awareness: The need for evidence-based framing strategies. *Government Information Quarterly*, 34(1), 1-7. Cybersecurity Glossary. National Initiative for Cybersecurity Careers and Studies. <https://niccs.cisa.gov/about-niccs/cybersecurity-glossary>.
- Carlton, M. (2016). Development of a cybersecurity skills index: A scenarios-based, hands-on measure of non-IT professionals' cybersecurity skills (Doctoral dissertation, Nova Southeastern University).
- Catota, F. E., Morgan, M. G., and Sicker, D. C. (2019). Cybersecurity education in a developing nation: the Ecuadorian environment. *Journal of Cybersecurity*, 5(1), tyz001.
- Cybersecurity and Infrastructure Security Agency. (2020). #Protect2020 Strategic Plan.
- Chowdhury, N. H., Adam, M. T. P., and Skinner, G. (2019). The impact of time pressure on cybersecurity behaviour: A systematic literature review. *Behaviour and Information Technology*, 38(12), 1290-1308.

- Chung, M. (2019). Why employees matter in the fight against ransomware. *Computer Fraud and Security*, 2019(8), 8–11.
- Conklin, A., and White, G. B. (2006, January). E-government and cyber security: the role of cyber security exercises. In *Proceedings of the 39th Annual Hawaii International Conference on System Sciences (HICSS'06)* (Vol. 4, pp. 79b-79b). IEEE.
- Costa, P., Montenegro, R., Pereira, T., and Pinto, P. (2019). The security challenges emerging from the technological developments: A practical case study of organizational awareness to the security risks. *Mobile Networks and Applications*, 24(6), 2032-2037. Retrieved from <http://search.ebscohost.com.ezhost.utrgv.edu:2048/login.aspx?direct=trueanddb=a9handAN=140064232andsite=ehost-live>
- Daengsi, T., Wuttidittachotti, P., Pornpongtechavanich, P., and Utakrit, N. (2021, June). A Comparative Study of Cybersecurity Awareness on Phishing Among Employees from Different Departments in an Organization. In *2021 2nd International Conference on Smart Computing and Electronic Enterprise (ICSCEE)* (pp. 102-106). IEEE.
- Dawson, J., and Thomson, R. (2018). The future cybersecurity workforce: going beyond technical skills for successful cyber performance. *Frontiers in Psychology*, 9, 744.
- Diaz, A., Sherman, A. T., and Joshi, A. (2020). Phishing in an academic community: A study of user susceptibility and behavior. *Cryptologia*, 44(1), 53-67.
- Fatokun, F. B., Hamid, S., Norman, A., and Fatokun, J. O. (2019, December). The impact of age, gender, and educational level on the cybersecurity behaviors of tertiary institution students: An empirical investigation on Malaysian universities. In *Journal of Physics: Conference Series*, 1339 (2019), p. 012098. IOP Publishing.
- Ford, W. D. (2021, March). Engaging Digital Natives with Simulations in a Business Data Security Course. In *Developments in Business Simulation and Experiential Learning: Proceedings of the Annual ABSEL conference* (Vol. 48).
- Habib, H., Naeini, P. E., Devlin, S., Oates, M., Swoopes, C., Bauer, L., ... and Cranor, L. F. (2018, August). User Behaviors and Attitudes Under Password Expiration Policies. In *SOUPS@ USENIX Security Symposium* (pp. 13-30).
- Halawi, L. A., McCarthy, R. V., and Pires, S. (2009). An evaluation of e-learning on the basis of Bloom's taxonomy: An exploratory study. *Journal of Education for Business*, 84(6), 374-380.
- Haney, J. M., and Lutters, W. G. (2021). Cybersecurity advocates: discovering the characteristics and skills of an emergent role. *Information and Computer Security*.

- Haney, J. M., and Lutters, W. G. (2017, July). Skills and Characteristics of Successful Cybersecurity Advocates. In *SOUPS*.
- Heartfield, R., and Loukas, G. (2018). Detecting semantic social engineering attacks with the weakest link: Implementation and empirical evaluation of a human-as-a-security-sensor framework. *Computers and Security*, 76, 101-127.
- Ikhsan, M. G., and Ramli, K. (2019, June). Measuring the information security awareness level of government employees through phishing assessment. In 2019 34th international technical conference on circuits/Systems, computers and communications (ITC-CSCC) (pp. 1-4). IEEE.
- Jacob, J., Peters, M., and Yang, T. A. (2019, June). Interdisciplinary Cybersecurity: Rethinking the Approach and the Process. In *National Cyber Summit* (pp. 61-74). Springer, Cham.
- Jibilian, I., and Canales, K. (2021, February 25). Here's a simple explanation of how the Massive SolarWinds hack happened and why it's such a big deal. Retrieved April 14, 2021, from <https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12>
- Kessler, G. C., and Ramsay, J. (2013). Paradigms for Cybersecurity Education in a Homeland Security Program. *Journal of Homeland Security Education*, 2(2013), 35-44.
- KnowBe4. (n.d.). KnowBe4 Philosophy. Retrieved April 2, 2021, from <https://www.knowbe4.com/about-us>.
- Krishna, B., and Sebastian, M. P. (2021). Examining the relationship between e-government development, nation's cyber-security commitment, business usage, and economic prosperity: a cross-country analysis. *Information and Computer Security*, 29(5), 737-760.
- Kweon, E., Lee, H., Chai, S., and Yoo, K. (2019). The utility of information security training and education on cybersecurity incidents: An empirical evidence. *Information Systems Frontiers*. <https://doi.org/10.1007/s10796-019-09977-z>
- Kortjan, N., and Solms, R. (2014). A conceptual framework for cybersecurity awareness and education in SA. *South African Computer Journal*. 52(52). doi:10.18489/sacj.v52i0.201
- Kostyuk, N., and Wayne, C. (2020). The microfoundations of state cybersecurity: Cyber risk perceptions and the mass public. *Journal of global security studies*. 0(2020), 1–25. <https://doi: 10.1093/jogss/ogz077>
- Kemper, G. (2019). Improving employees' cybersecurity awareness. *Computer Fraud and Security*, 2019(8), 11-14. doi:10.1016/S1361-3723(19)30085-5



- Macmanus, S., Caruson, K. and Mcphee, B. (2013) Cybersecurity at the Local Government Level: Balancing Demands for Transparency and Privacy Rights. *Journal of Urban Affairs*, 35(4), 451-470, DOI: 10.1111/j.1467-9906.2012.00640.x
- Matthews, T. (2012). Passwords are not enough. *Computer Fraud and Security*, 2012(5), 18-20.
- McCormac, A., Calic, D., Butavicius, M., Parsons, K., Zwaans, T., and Pattinson, M. (2017). A reliable measure of information security awareness and the identification of bias in responses. *Australasian Journal of Information Systems*, 21. doi:10.3127/ajis.v21i0.1697
- Medlin, B. D., Cazier, J. A., and Foulk, D. P. (2008). Analyzing the vulnerability of US hospitals to social engineering attacks: how many of your employees would share their password? *International Journal of Information Security and Privacy (IJISP)*, 2(3), 71-83.
- Miller, J. N. (2017). 2017 user risk report: Results of an international cybersecurity awareness survey. *Wombat Security Technologies*.
- Moramarco, S. (2020). How to create a human firewall: Top 7 elements required for success in 2018. *Infosec Resources*. <https://resources.infosecinstitute.com/topic/how-to-create-a-human-firewall-top-7-elements-required-for-success-in-2018/>.
- Mouheb, D., Abbas, S., and Merabti, M. (2019). Cybersecurity curriculum design: A survey. In *Transactions on Edutainment XV* (pp. 93-107). Springer, Berlin, Heidelberg.
- Nam, T. (2019). Understanding the gap between perceived threats to and preparedness for cybersecurity. *Technology in society*, 58, 101122.
- Ng, A. (2019, December 5). Ransomware froze more cities in 2019 as hackers got smarter. Retrieved January 6, 2020, from <https://www.cnet.com/news/ransomware-devastated-cities-in-2019-officials-hope-to-stop-a-repeat-in-2020/>.
- NIST Cybersecurity Framework. National Institute of Standards and Technology; U.S. Department of Commerce: Gaithersburg, MD (16 April 2018).
- Oancea, R., Bârsan, G., and Giurgiu, L. (2019). Approach on increasing user security awareness. Paper presented at the *International Conference Knowledge-Based Organization*, 25(3) 46-50.
- Olmstead, K., and Smith, A. (2017a). Americans and cybersecurity. *Pew Research Center*, 26, 311-327. Research Center, 26, 311-327.
- Olmstead, K., and Smith, A. (2017b). What the public knows about cybersecurity. *Pew Research Center*, 22.
- Oxford Analytica. (2021). US pipeline hack signals critical infrastructure risks. *Emerald Expert Briefings*, (oxan-es).

- Peker, Y. K., Ray, L., Da Silva, S., Gibson, N., and Lamberson, C. (2016). Raising cybersecurity awareness among college students. *Journal of the Colloquium for Information System Security Education (CISSE)*, 4(01)
- Redekop, B. D. (2021). IT Security training and awareness in the multigenerational workplace. *International Journal of Information Security and Cybercrime (IJISC)*, 10(2), 9-15.
- Ricci, J., Breiting, F., and Baggili, I. (2019). Survey results on adults and cybersecurity education. *Education and Information Technologies*, 24(1), 231-249.
- Salgues, B. (2016). 4 - acceptability and diffusion. In B. Salgues (Ed.), *Health industrialization* (pp. 53-69) Elsevier. doi:<https://doi.org/10.1016/B978-1-78548-147-5.50004-7> Retrieved from <https://www.sciencedirect.com/science/article/pii/B9781785481475500047>
- Salunke M. D, Kumbharkar P. B, and Dr. Pramod Kumar. (2021). A proposed methodology to mitigate the ransomware attack. In *Recent Trends in Intensive Computing*, 16-21. IOS Press.
- Schürmann, C., Jensen, L. H., and Sigbjörnsdóttir, R. M. (2020). Effective Cybersecurity Awareness Training for Election Officials. Paper presented at the Electronic, 196-212.
- Sherif, E., Furnell, S., and Clarke, N. (2015, August). An identification of variables influencing the establishment of information security culture. In *International Conference on Human Aspects of Information Security, Privacy, and Trust* (pp. 436-448). Springer, Cham.
- Skertic, J. (2021). Cybersecurity Legislation and Ransomware Attacks in the United States, 2015–2019 (Doctoral dissertation, Old Dominion University).
- Spremić, M., and Šimunic, A. (2018, July). Cyber security challenges in digital economy. In *Proceedings of the World Congress on Engineering* (Vol. 1, pp. 341-346). Hong Kong, China: International Association of Engineers.
- Tirumala, S. S., Sarrafzadeh, A., and Pang, P. (2016, December). A survey on Internet usage and cybersecurity awareness in students. In *2016 14th Annual Conference on Privacy, Security, and Trust (PST)* (pp. 223-228). IEEE.
- Tirumala, S. S., Valluri, M. R., and Babu, G. A. (2019, January). A survey on cybersecurity awareness concerns, practices, and conceptual measures. In *2019 International Conference on Computer Communication and Informatics (ICCCI)* (pp. 1-6). IEEE.
- Vishwanath, A. (2021, May 13). Opinion: The failures that led to the colonial pipeline ransomware attack. CNN. Retrieved April 20, 2022, from <https://www.cnn.com/2021/05/13/opinions/colonial-pipeline-ransomware-attack-was-stoppable-vishwanath/index.html>

- Walsh, M. (2020). Implement multi-factor authentication on all federal systems now. *Student Papers in Public Policy*, 2(1), 3.
- Weber, J. E., Guster, D., Safonov, P., and Schmidt, M. B. (2008). Weak password security: An empirical study. *Information Security Journal: A Global Perspective*, 17(1), 45-54.
- Wilson, L. O. (2016). Anderson and Krathwohl–Bloom’s taxonomy revised. *Understanding the New Version of Bloom's Taxonomy*.
- Yazdanpanahi, B. (2021). Steps in Building a Successful Resilient Cyber Protocol. *Certified Public Manager® Applied Research*, 2(1), 5.
- Young, A. and Yung, M. (2017). Cryptovirology: The birth, neglect, and explosion of ransomware. *Communications of the ACM*. 60(7). 24-26. 10.1145/3097347.
- Zimba, A., Wang, Z., Chen, H., and Mulenga, M. (2019). Recent advances in cryptovirology: State-of-the-art crypto mining and crypto-ransomware attacks. *KSII Transactions on Internet and Information Systems (TIIS)*, 13(6), 3258-3279.
- Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., and Basim, H. N. (2020). Cybersecurity awareness, knowledge, and behavior: A comparative study. *Journal of Computer Information Systems*, 1-16.

## APPENDIX A

## APPENDIX A

### CYBERSECURITY AWARENESS SURVEY (ADAPTED FROM THE PEW RESEARCH CENTER'S (2016) CYBERSECURITY KNOWLEDGE QUIZ).

\* 1. Please enter your name and e-mail address, to ensure you are given credit for completing your training.

Name

Email Address

#### I. Demographic Information (Questions 1-9)

\* 2. Have you ever taken a cybersecurity or internet safety course before this one?

- ☐ I don't know
- ☐ Yes
- ☐ No

\* 3. How many years with Cameron County?

- ☐ 0 - 5 years
- ☐ 6 - 10 years
- ☐ 11 - 15 years
- ☐ 16 - 20 years
- ☐ 21 - 25 years
- ☐ 26 – 30 years

- ☐ 30 years and above

\* 4. Please state your ethnicity

- ☐ American Indian or Alaska Native.
- ☐ Asian.
- ☐ Black or African American.
- ☐ Native Hawaiian or Other Pacific Islander.
- ☐ White
- ☐ Hispanic or Latino

\* 5. Please state your gender.

- ☐ Male
- ☐ Female
- ☐ Prefer not to answer

\* 6. Please select your age range

- ☐ 18 to 25
- ☐ 26 to 35
- ☐ 36 to 45
- ☐ 46 to 55
- ☐ 56 and older

\* 7. What is your Highest Educational Degree held?

- ☐ H.S. Diploma / GED
- ☐ Associates
- ☐ Bachelors
- ☐ Masters
- ☐ Doctorate
- ☐ Not applicable

\* 8. What is your primary language spoken?

- ☐ English
- ☐ Spanish
- ☐ Other

\* 9. How would you rate your technical skills?

- ☒ Basic knowledge - You have a common knowledge or an understanding of basic computer concepts.
- ☐ Limited experience - You have experience gained experience on the job. You are expected to need help when performing technical tasks.
- ☐ Intermediate knowledge - You can successfully complete computer tasks as requested.
- ☐ Advanced knowledge - You can perform work on your computer without assistance.
- ☐ Expert Knowledge - You are known as an expert in this area. You can guide co-workers.

\* 10. What department are you considered to work under at Cameron County?

- ☒ Administration
- ☐ Law Enforcement
- ☐ Elected Official's Office
- ☐ Health-Related department
- ☐ Judicial or Court related
- ☐ Road/Bridge/Maintenance
- ☐ Auditors Office
- ☐ Engineering and DOT
- ☐ District Attorney
- ☐ Parks and Recreation
- ☐ Pre-Trial
- ☐ Probation
- ☐ Veterans Department
- ☐ Purchasing
- ☐ Information Technology
- ☐ Commissioner's Court
- ☐ Other (please specify)



## II. Knowledge of Cybersecurity Issues (Questions 10-21)

\* 11. What does the “HTTPS://” at the beginning of a URL denote, as opposed to "HTTP://" (without the “s”)?

- ☐ That the site has special high definition
- ☐ That information entered into the site is encrypted
- ☐ That the site is the newest version available
- ☐ That the site is not accessible on certain computers
- ☐ None of the above
- ☐ Not sure

\* 12. How do viruses and malware get into your computer?

- ☐ Files from a USB stick
- ☐ E-mail attachments
- ☐ Spam e-mail links
- ☐ Websites
- ☐ All of the Above
- ☐ Not sure

\* 13. Which of the following is an example of a “phishing” attack?

- ☐ Sending someone an email that contains a malicious link that is disguised to look like an email from someone the person knows
- ☐ Creating a fake website that looks nearly identical to a real website in order to trick users into entering their login information

☐ Sending someone a text message that contains a malicious link that is disguised to look like a notification that the person has won a contest

☐ All of the above

☐ Not sure

\* 14. A group of computers that are networked together and used by hackers to steal information is called a ...

☐ Botnet

☐ Rootkit

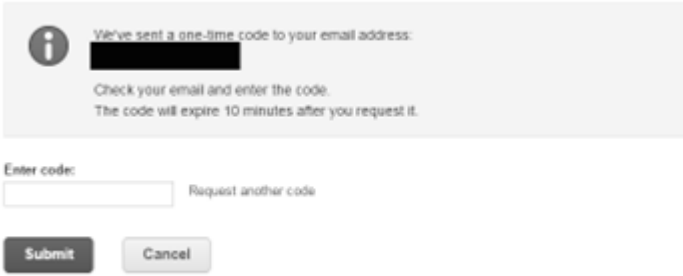
☐ DDoS

☐ Operating system


☐ Not sure

\* 15. Some websites and online services use a security process called two-step authentication. Which of the following images is an example of two-step authentication?

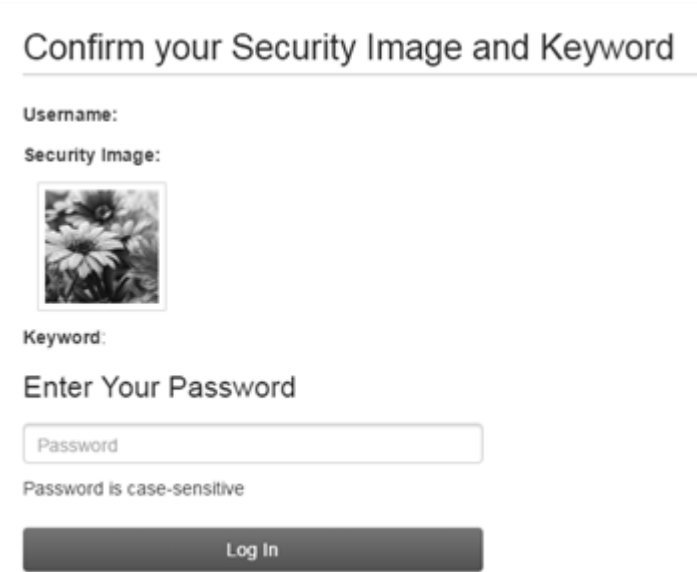
☐



☐



☐



- ☐ None of these
- ☐ Not sure

\* 16. Which of the following four passwords is the most secure?

- ☐ Boat123
- ☐ WTh!5Z
- ☐ into\*48
- ☐ 123456
- ☐ Not sure

\* 17. Criminals access someone's computer and encrypt the user's personal files and data. The user is unable to access this data unless they pay the criminals to decrypt the files. This practice is called ...

- ☐ Botnet
- ☐ Ransomware
- ☐ Driving
- ☐ Spam
- ☐ None of the above
- ☐ Not sure

\* 18. "Private browsing" is a feature in many internet browsers that lets users access web pages without any information (like browsing history) being stored by the browser. Can internet service providers see the online activities of their subscribers when those subscribers are using private browsing?

- ☐ Yes
- ☐ No
- ☐ Not sure

\* 19. Turning off the GPS function of your smartphone prevents any tracking of your phone's location.

- ☐ True
- ☐ False
- ☐ Not sure

\* 20. What kind of cybersecurity risks can be minimized by using a Virtual Private Network (VPN)?

- ☐ Use of insecure Wi-Fi networks
- ☐ Key-logging
- ☐ De-anonymization by network operators
- ☐ Phishing attacks
- ☐ Not sure

\* 21. If a public Wi-Fi network (such as in an airport or café) requires a password to access, is it generally safe to use that network for sensitive activities such as online banking?

- ☐ Yes, it is safe
- ☐ No, it is not safe
- ☐ Not sure

## APPENDIX B

## APPENDIX B

### SAMPLE OF INITIAL E-MAIL NOTIFICATION

 The linked image cannot be displayed. The file may have been moved, renamed, or deleted. Verify that the link points to the correct file and location.

Cameron County Employees,

In 2019, the Texas Legislature enacted House Bill 3834 which mandates cybersecurity training for local government employees. As a result, any employee, including elected officials, who use a computer for at least 25 percent of their time to complete their duties, is required to complete the training.

In order to complete the necessary training, each employee will receive an email from the Security Education Platform, an example of the email is displayed below. This is a legitimate email and will include a link to access the required training.

Please complete the assigned training by June 14, 2021, since the IT Department is required to submit documentation that we have complied with the requirements. If you do not receive the email from the

Security Education Platform by April 23, 2020, please contact our department at 956-544-0818 or send us an email at [helpdesk@co.cameron.tx.us](mailto:helpdesk@co.cameron.tx.us).

Please complete the Cameron County Cybersecurity Survey by clicking the following link:

<https://www.surveymonkey.com/r/G6YGGPF>



The linked image cannot be displayed. The file may have been moved, renamed, or deleted. Verify that the link points to the correct file and location.

**Contact Information:**

Office Phone: (956)544-0818

Email: [helpdesk@co.cameron.tx.us](mailto:helpdesk@co.cameron.tx.us)



The linked image cannot be displayed. The file may have been moved, renamed, or deleted. Verify that the link points to the correct file and location.

Cameron County Information Technology Department | (956) 544-0818 | 835 E. Levee, Brownsville, Texas  
78520



## APPENDIX C

## APPENDIX C

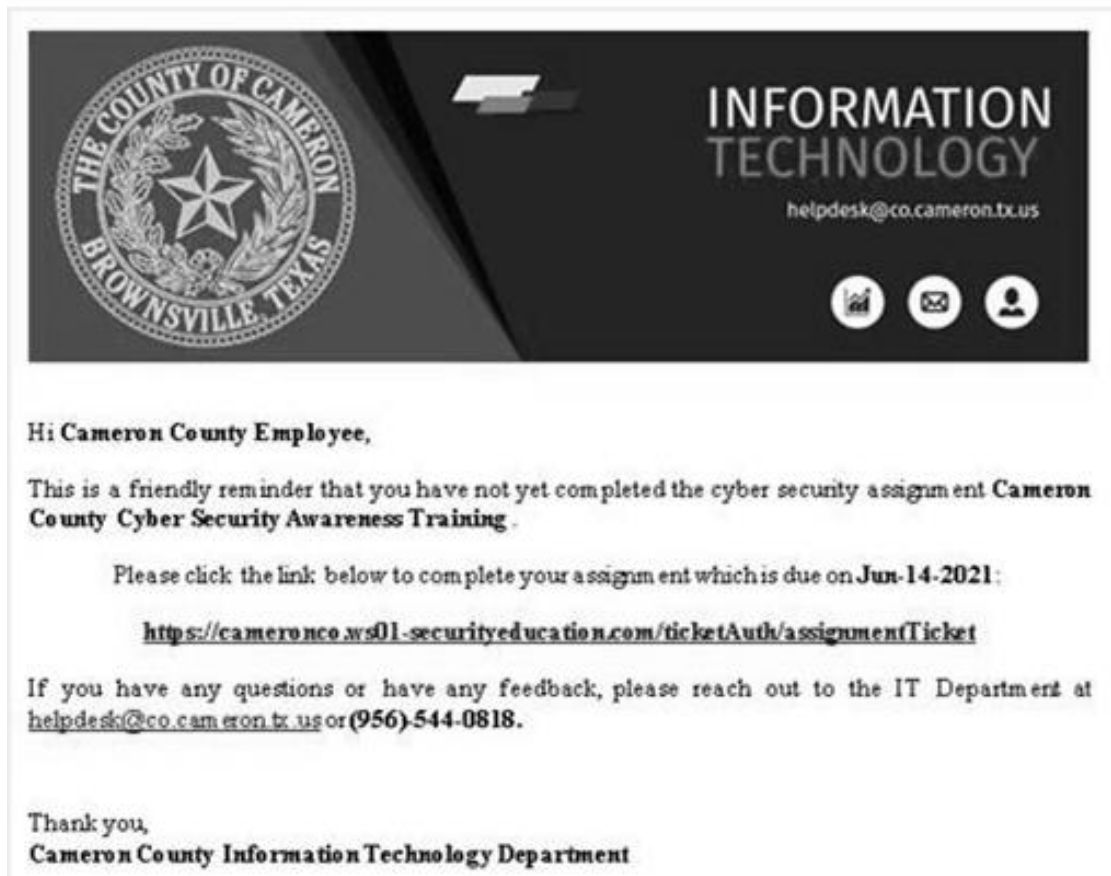
### EMPLOYEE REMINDERS FOR COMPLETION OF TRAINING



## APPENDIX D

## APPENDIX D

### SCREENSHOT OF THE EMAIL FROM THE SECURITY EDUCATION PLATFORM



## BIOGRAPHICAL SKETCH

Juan Jaime Saldana II was born on October 3, 1976 in Yuma, Arizona. The eldest son among the two children of Mr. Jaime Saldana Sr. and Mrs. Gloria E. Hunter. He attained his Bachelor of Science in Computer Science degree in 1999 at the then University of Texas at Brownsville (UTB) after raising his two daughters he returned to school and obtained a Master's in Education and e-Learning in 2014 and followed that up with a Doctorate in Curriculum and Instruction with a focus on Instructional Technology from the now University of Texas Rio Grande Valley (UTRGV) in 2023. In those two decades, he has worked in the Information Technology field, most currently for Cameron County as their Chief of Technology. He is also a member of the Kappa Delta Pi Omicron Eta Chapter at UTRGV.

Professionally Mr. Saldana worked for 15 years as the MIS Manager for the local Keppel AmFELS shipyard, a subsidiary of the Singaporean-based Keppel Offshore and Marine. There he attended the Keppel Young Leaders Management Academy at Nan Yang Technical University in Singapore. This was followed by an opportunity in 2016 to join the team at Cameron County and help to modernize local government processes as their Chief Technology Officer. In 2017, to develop his instructional skills, he decided to share his knowledge and experience with the next generation of up-and-coming information technology professionals by joining the CIS department at Texas Southmost College as an Adjunct professor.

**Contact Information:** 5451 Cedar Trail Dr. Brownsville, TX. 78526 [jsaldana2@msn.com](mailto:jsaldana2@msn.com)