Walden University
ScholarWorks

Walden Dissertations and Doctoral Studies

Walden Dissertations and Doctoral Studies Collection

2021

User Awareness and Knowledge of Cybersecurity and the Impact of training in the Commonwealth of Dominica

Jermaine Jewel Jean-Pierre
Walden University

Walden University

College of Management and Technology

This is to certify that the doctoral dissertation by

Jermaine Jewel Jean-Pierre

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

Review Committee
Dr. Branford McAllister, Committee Chairperson, Management Faculty
Dr. Danielle Wright-Babb, Committee Member, Management Faculty
Dr. David Bouvin, University Reviewer, Management Faculty

Chief Academic Officer and Provost
Sue Subocz, Ph.D.

Walden University
2021

Abstract

User Awareness and Knowledge of Cybersecurity and the Impact of training in the Commonwealth of Dominica

by

Jermaine Jewel Jean-Pierre

MBA, Midwestern State University, 2008

BA, University of the Virgin Islands, 2000

Dissertation Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Philosophy

Management

Walden University

June 2021

Abstract

The frequency of cyberattacks against governments has increased at an alarming rate and the lack of user awareness and knowledge of cybersecurity has been considered a contributing factor to the increase in cyberattacks and cyberthreats. The purpose of this quantitative experimental study was to explore the role and effectiveness of employee training focused on user awareness of cyberattacks and cybersecurity, with the intent to close the gap in understanding about the level of awareness of cybersecurity within the public sector of the Commonwealth of Dominica. The theoretical framework was Bandura's social cognitive theory, following the idea that learning occurs in a social context with a reciprocal interaction of the person, environment, and behavior. Data were collected using a questionnaire modified to collect demographic information for a pretest and a posttest analysis. Data analysis using a *t* test and multiple linear regression was conducted to test the hypotheses related to factors affecting user awareness and knowledge of cybersecurity. Results indicated that participants who were part of the experimental group showed higher knowledge of cybersecurity after the posttest and that demographic factors were not significant predictors of cybersecurity awareness and knowledge. The findings may be used to empower employees with knowledge of cybersecurity and increase awareness within the public sector, and to protect the information systems from cybersecurity threats. The findings may lead to positive social change by encouraging other stakeholders to discuss how risks associated with cybersecurity can be mitigated to enhance service effectiveness.

User Awareness and Knowledge of Cybersecurity and the Impact of training in the

Commonwealth of Dominica

by

Jermaine Jewel Jean-Pierre

MBA, Midwestern State University, 2008

BA, University of the Virgin Islands, 2000

Dissertation Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Philosophy

Management

Walden University

June 2021

Dedication

This doctoral work is dedicated to my father, Mr. Elmo Boysie Thomas, and my aunt, Rachel Jean-Pierre-Leslie who passed away from cancer before I could complete this journey. No matter how difficult the goal seemed to be, their confidence was my inspiration to move forward and press on.

Acknowledgments

I give all the praises to God for his unconditional love and guidance. A special thank you to my mother Dr. Linda Thomas, my sister, Michelle Thomas, my brothers Olson Forde Senior, and Kareem Thomas, my niece Oneiqua Forde, and my goddaughter Orina Faith Bruno. Thank you all for encouraging me at every opportunity to finish this major endeavor in my life and for the love and support that you have shown to me always.

To my Aunty Irma Edwards for your source of knowledge, encouragement, and assistance throughout this journey. You have never given up on me. Thank you to my friends Fabrina Bruno, and Grell Francis for your assistance and words of encouragement. Thank you to my prayer team, Jemima Charles, Juliet Lewis, Neva Edwards, Lundell Edwards, and John Lewis.

It is also with deepest gratitude and warmest affection that I say thank you to my Committee Chair, Dr. Branford McAllister for your never-ending support, encouragement, and wisdom during this entire dissertation process. There are not enough words to express my gratitude to you. Thank you for the insights and attention to details. Thank you, Dr. Danielle L. Wright-Babb and Dr. David Bouvin, for the helpful comments and support.

Finally, I would like to thank all of the family, friends, Government of the Commonwealth of Dominica, and Walden staff who contributed to the success of this dissertation.

Table of Contents

List of Tables

List of Figures

Chapter 1: Introduction to the Study

Over the last 5 years, the security of information has become a concern to many governments around the world including the Commonwealth of Dominica (Aguinaldo, 2018). The frequency of cyberattacks against governments has increased at an alarming rate (Ross et al., 2018). Recent government data breaches, including within the Federal Emergency Management Agency (FEMA), have created an anxiety in governments who see the need to protect their data and information from cyberattacks that can cause irreparable damage to their operations (Aguinaldo, 2018; Bystrova, 2017). Further, the use of the internet and connected information systems has posed significant challenges for governments around the world because misuse by employees has led to vulnerability to cyberattacks (Aguinaldo, 2018; Digrazia, 2018; Ross et al., 2018). The challenges are even greater for developing countries such as the Commonwealth of Dominica because of fewer cybersecurity technical resources and professionals (Organization of American States [OAS], 2018). Notwithstanding, technology has become increasingly essential in the everyday activities of the public sector of the Commonwealth of Dominica and therefore this study was needed since the results may contribute to the understanding of cybersecurity and lead to policies to support and protect information and new technologies within the public sector.

This chapter includes the background of my research which focused on user awareness of cyberattacks and cybersecurity. Additionally in the chapter, I address the problem statement, the purpose of the study, the research questions, and hypotheses. I discuss the theoretical framework for this study, the nature of the study, definitions, assumptions, scope and delimitations, limitations, and the significance of the study.

Background of the Study

Dadkhah et al. (2018) stated that hackers often exploit vulnerabilities in information systems by manipulating data, destroying systems by using the backdoor created by the employees who accessed unauthorized websites containing viruses and malwares. These actions of accessing unauthorized websites containing viruses and malwares are attributed to employees’ lack of awareness of cybersecurity, which exposes the information systems to sophisticated internet security risks (Jones & Shashidhar, 2017; Krishan, 2018). In a cybersecurity report, the OAS (2016) identified the public sector of the Commonwealth of Dominica as being generally unaware of cyberthreats. The report further stated that users do not have an adequate awareness of the use of the Internet and thus, are unable to mitigate against a cyberattack.

Employees in governments have been a source of vulnerabilities to their information systems and network infrastructure. Further, employees’ lack of awareness has been listed as a reason for network intrusions (Safa et al., 2016). Eliminating the behavior of employees that is considered risky is critical for the enhancement of the cybersecurity of any government (Safa et al., 2016). Cybersecurity breaches have been increasing over the years with frequent attacks in the last 2 years (Central Intelligence Agency, 2015; United States Securities and Exchange Commission, 2015). Intrusion into the information system of a government can have dire consequences especially when information communication technology can reduce the cost of operations and increase the efficiency of service delivery in most governments (O'Driscoll, 2018).

In 2013, the government of the Commonwealth of Dominica, as part of its public sector transformation efforts, increased communication to its citizens and customers virtually through its network communications (Edwards, 2013). The network communication systems have allowed the public sector to increase its rate of doing business and provision of service thus changing the way in which information and data are exchanged. However, the increased use of information systems and the internet has increased the risks of cyberthreats and cybercrimes within the public sector of the Commonwealth of Dominica.

The public sector of the Commonwealth of Dominica has introduced several eGovernment services, including online birth registration and electronic tax filing. Availability of those services through eGovernment portals has created a backdoor to risk of cyberattacks to its databases as well as other infrastructure. An attack on those systems can have a negative impact on the public sector of the Commonwealth of Dominica’s adoption of eGovernment to reduce operational cost and improve its service delivery (Vogel, 2016).

Over the years, cyberthreats have evolved from simple viruses to attacks that can cripple an entire government’s information system (Lee et al., 2016). The strategies employed and the sophistication of the cyberattacks are disguised to the extent that it is difficult to identify by employees. As a result of its dependency on the use of the internet and information system to provide critical government services, the public sector of the

Commonwealth of Dominica is concerned about the protection of its information systems.

According to informal reports from the Information and Communication Technology Unit of the Commonwealth of Dominica and the National Telecommunication Regulatory Commission (NTRC, 2015) of the Commonwealth of Dominica, the increase in the use of the internet has resulted in over 10 reported cases of ransomware attacks. Given the increased use of the internet, the number of attacks may have increased since that time due to the widespread increase in attacks globally.

In the scholarly literature, an emphasis has been placed on data security despite the constant risks of cyberattacks faced by governments due to the lack of awareness and knowledge of employees (Bauer & Bernroider, 2017). The academic research on employee awareness and knowledge of cybersecurity and the impact of training in the public sector of the Commonwealth of Dominica is very limited. Few government official documents have referred to cybersecurity and even fewer international organizations responsible for cybersecurity within the region have developed any official plan of action for dealing with employee awareness and knowledge of cybersecurity (Safa et al., 2016). The general consensus in the scholarly literature is that information security training should be standard practice as the most common approach to increasing employee knowledge of cyberattacks and cybersecurity (Bauer & Bernroider, 2017).

While there has been ample coverage of cyber vulnerabilities of networked systems in the scholarly research and literature, several gaps are evident especially relating to employee cybersecurity awareness and the management of information and communication technology in the public sector of the Commonwealth of Dominica (see Digrazia, 2018; Niemimaa & Niemimaa, 2017). Additionally, the process of developing and transferring cybersecurity knowledge remains vague due to the lack of available research on information security training on employee awareness and knowledge of cybersecurity (Digrazia, 2018). A documented cause of cybersecurity vulnerability is a lack of employee awareness, yet there is a lack of research into the causes and remedies of employee cybersecurity awareness. Training may be effective, but there is no research about the effectiveness of training in cybersecurity awareness. In addition to this, there has been marginal research on the cybersecurity position of governments in the region. Most of the recent research on cybersecurity has been done on developed countries. The type of training that influences cybersecurity awareness and knowledge training have not yet been explored by researchers. Further, the scholarly research has not agreed on a concrete methodology on how to evaluate the various types of cybersecurity awareness and knowledge training (Haeussinger & Kranz, 2017).

Consequently, there is little empirical evidence to assess how the level of awareness and knowledge can influence attitudes and behaviors in the use of the internet in the public sector of the Commonwealth of Dominica. This study was needed to fill the gap in research and to increase the knowledge about cybersecurity among employees within the public sector, especially the government of the Commonwealth of Dominica.

Problem Statement

The social problem addressed in this study was that the lack of awareness of cybersecurity by employees within the public service and government agencies in the

Commonwealth of Dominica created conditions in which cyberattacks are doing harm to the information systems (Aguinaldo, 2018; Alavi & Leidner, 2001; Skarga-Bandurova et al., 2016). Research on cybersecurity and security in general had revealed that in organizations' attempts to manage security efforts, the weakest element is human (Veiga, 2016). Stevens (2018) believed that to mitigate against cybersecurity threats in an organization, it is necessary to have employees who can take actions to prevent threats through their awareness and knowledge of cybersecurity. However, in spite of the research into cybersecurity awareness, there is little or no research documented in the scholarly literature that quantifies the level of awareness of cybersecurity, or that pertains to the specific role that employee training plays in the awareness of cybersecurity in the public sector of the Commonwealth of Dominica. Therefore, the research problem was the lack of knowledge and understanding of the level of awareness of cybersecurity and the role and effectiveness of employee training to enhance cybersecurity. The consequence of that gap is the inability of the government to develop and implement policies and procedures leading to more effective cybersecurity.

Purpose of the Study

The purpose of this quantitative experimental study was to explore the role and effectiveness of employee training focused on user awareness of cyberattacks and cybersecurity, with the intent to close the gap in understanding about the level of awareness of cybersecurity within the public sector of the Commonwealth of Dominica. The target population of this experimental study consisted of employees within the public sector of the Commonwealth of Dominica. I used a pretest, posttest controlled experimental design. The employees participating in the study were divided into a control group and an experimental group. The experimental group participated in a cybersecurity awareness training. The dependent variable (DV) was the score on a test of awareness and knowledge of cybersecurity and the independent variables (IVs) were time (pretest and posttest) and group (control and experimental). There were also four demographic variables: age, gender, location, and access to the internet.

This study may promote positive social change by increasing understanding within the public sector of the Commonwealth of Dominica about employee awareness and the benefits of training in increasing their awareness of cybersecurity. Contribution to the prevention of cyberattacks and increase in the confidence of the employees in the public sector in using its information systems may influence behavior change in the use of the internet on employees' own devices and minimize risks to personal data and information which could impact individuals financially, culturally, and otherwise. Employees are part of families and communities and could also influence behavior change within the wider society in the use of both private and personal information systems.

Research Questions (RQs) and Hypotheses

Researchers have not yet concluded how threats influence users' behaviors or how best to improve the security practices of the users (Jenab & Moslehpour, 2016). The purpose of this quantitative experimental study was to close the gap in understanding about the level of awareness of cybersecurity within the public sector of the

Commonwealth of Dominica and the role and effectiveness of employee training focused on user awareness of cyberattacks and cybersecurity.

RQ1: What is the level of cybersecurity awareness and knowledge in the public sector of the Commonwealth of Dominica?

This research question was intended to establish through descriptive statistics a quantified baseline understanding of the level of cybersecurity awareness (i.e., prior to any training) for all participants, and to identify any differences between the two groups. In addition, the following hypotheses were tested to establish a baseline difference between the two groups (control and experimental):

$H_0$1. There is no difference in the level of knowledge and use of cybersecurity between the control and experimental groups during the pretest.

H_a1$_.$ There is a difference in the level of knowledge and use of cybersecurity between the control and experimental groups during the pretest.

RQ2: What is the pretest level of cybersecurity awareness and knowledge according to demographic factors age, gender, location, and access to the internet in the public sector of the Commonwealth of Dominica?

$H_0$2. There is no difference in the pretest level of cybersecurity awareness and knowledge according to demographic factors age, gender, location, and access to the internet in the public sector of the Commonwealth of Dominica.

H_a2. There is a difference in the pretest level of cybersecurity awareness and knowledge according to at least one of the demographic factors of age, gender, location, and access to the internet in the public sector of the Commonwealth of Dominica.

RQ3: Does a training intervention impact the level of knowledge and use of cybersecurity?

$H_0$3. The experimental group demonstrates a level of knowledge and use of cybersecurity equal to or lower than the control group as measured during the posttest.

H_a3$_.$ The experimental group demonstrates a higher level of knowledge and use of cybersecurity than the control group as measured during the posttest.

RQ4: Is there a change or increase in the level of knowledge and use of cybersecurity for the experimental group from the pretest to the posttest?

$H_0$4. There is no change or a decrease in the level of knowledge and use of cybersecurity for the experimental group from the pretest to the posttest.

H_a4$_.$ There is an increase in the level of knowledge and use of cybersecurity for the experimental group from the pretest to the posttest.

Theoretical Foundation

Bandura (1986) developed the social cognitive theory (SCT) in 1986 and posited that learning occurs in a social context with a reciprocal interaction of the person, environment, and behavior. The general idea behind SCT is the emphasis that is placed on social influence and the need for external and internal social reinforcement. The SCT takes into consideration the unique way in which an individual acquires knowledge as well as the way in which the past experiences of individuals determine whether specific behavioral action will occur. Bandura (1986) described an individual as having the capabilities to execute a course of action that is required to attain a desired objective. In the context of this research, the appropriate use of the internet by employees may be influenced by their interest and ability to learn more about cybersecurity through targeted and continuous training.

There have been many theories over the years that explained the developmental changes that people endure over the course of their lives. The theories differ in how people adapt to changes and the mechanism employed to motivate and deal with the behavior of people. The theories have focused primarily on the growth capabilities especially during the period of when change can rapidly occur.

The social and economic changes that occur in life are often a direct result of innovations in technology. Technological changes have altered the life events that are customary in society today. Attention is often focused on the threats and vulnerabilities likely to originate from sources external to the organization. However, a significant percentage of cyberthreats originate from inside the organization (Andrews & Gotz, 2013). Employees are a threat to the organization’s information systems when they engage in behaviors that are counterproductive to the information system policies of the organization. The core concepts that are associated with SCT and considered to be important in influencing behavior include observational learning/modeling, organizational facilitators, self-efficacy, and self-regulation (Bandura, 2001).

Nature of the Study

I used a quantitative comparative methodology for this research. Quantitative researchers investigate a phenomenon by gathering data that is quantifiable to test a hypothesis about a relationship between variables (Claydon, 2015). The purpose of my research was to understand the level of employee awareness of cybersecurity, and to explore the role and effectiveness of employee training focused on user awareness of cyberattacks and cybersecurity, with the intent to close the gap in understanding about the level of awareness of cybersecurity within the public sector of the Commonwealth of Dominica. Therefore, a quantitative method was appropriate. A qualitative method was not considered appropriate since qualitative researchers develop a subjective view of the behavior of a population in relation to its experiences or decision-making processes and its association with a phenomenon (see Newman & Hitchcock, 2011).

The research was done using a pre- and posttest quantitative research design. The groups were formed using random sampling with stratification on the two variables of age and gender of the participants within the public sector of the Commonwealth of Dominica. Both groups, the control group and the experimental group, were given a pretest. The experimental group was then given cybersecurity training for a period of 4 weeks. I sought the assistance of the Public Service Training Center in administering the training. The training was conducted by a lecturer from the pool of Information and Communication Technology (ICT) lecturers from the Public Service Training Center. The posttest was repeated to both the control group and the experimental group from within the public sector of the Commonwealth of Dominica. The research design was two-group pretest-posttest design. In a two-group pretest posttest design, the DV is measured once prior to the implementation of the treatment and then measured once again after the treatment is implemented (Creswell, 2013). Comparisons were made between the groups twice: during the pretest and during the posttest. A comparison was also made for the experimental group between the pretest and the posttest. Hypotheses for RQ1 and RQ3 were tested using an independent samples *t* test. Hypothesis for RQ2 was evaluated using multiple linear regression (MLR). Hypothesis for RQ4 was evaluated using a paired *t* test.

Definitions

Cyberattack: A malicious and deliberate action with the purpose of disrupting or compromising the operation of a computer network or the information stored in an information system (Dykstra & Spafford, 2018).

Cybersecurity: The training, policies, and technology that is designed to ensure the protect the cyber environment (Hadlington, 2017).

Cyberthreat: A malicious act with the purpose of damaging or stealing data from an organization that causes disruption to the digital life (Hadlington, 2017).

External Threats: Threats originating externally to the organization. These threats include past employees, hackers, natural disasters, and other government agencies (Kshetri, 2013).

Internal Threats: Threats originating from within the organization. The threats include employees, contractors, and managers who have been trusted with access to the information systems (Ahmad et al., 2015).

Ransomware: Extorting money from victims using a form of cryptovirology (Ferrillo & Singer, 2015).

Security Practice: The behavior that is exhibited by the adoption of security technology and an awareness of security behaviors related to the use of the internet and computers (Ferrillo & Singer, 2015).

Assumptions

An assumption is something that is considered outside the control of the researcher and would cause the research to be irrelevant if the assumption was not present (Leedy & Ormrod, 2010). Several assumptions were critical to this research:

- The employees of the public sector in the Commonwealth of Dominica would have participated in testing truthfully and that the data was reliable.
- The sample data was a representative of the population of the public service of the Commonwealth of Dominica.
- The sample population had basic computer skills to adequately perform in the training course.
- Enough employees of the public sector of the Commonwealth of Dominica were interested and available to participate in the training program to meet the calculated minimum sample size.

Scope and Delimitations

Delimitations are the characteristics of the research that limit the scope and define the boundaries of the study (Willan, 2016). Delimitations are within the control of the researcher and include factors that focus the research questions, variables, and theoretical perspectives. Delimitations in a study can influence the interpretation of the results of the study as well as establish the parameters of the study (Willan, 2016). Delimitations also assist in limiting the scope of the research (Oravec, 2017).

The purpose of this quantitative experimental study was to close the gap in understanding about the level of awareness of cybersecurity within the public sector of the Commonwealth of Dominica and the role and effectiveness of employee training focused on user awareness of cyberattacks and cybersecurity. The study was delimited to the population of the public sector of the Commonwealth of Dominica. The public sector is defined as a body of employees working within central government including temporary, permanent, nonestablished employees, and contractual officers, as well as employees of statutory corporations, quasigovernment agencies, and parastatal institutions. This delimitation excluded participants from the private sector of the Commonwealth of Dominica. The theoretical framework for the study was limited to the SCT and its relationship to the use of the internet by employees who have been influenced to learn more about cybersecurity through targeted and continuous training. The study provided to the public sector of the Commonwealth of Dominica a baseline understanding of the level of awareness that currently exists. However, the study did not make provision for a similar transfer of knowledge to any future employees of the public sector of the Commonwealth of Dominica. The study was also delimited in that the research did not measure whether the employees complied with the computer security policies where they work. The training did not make provision for observing the employees at their workstations.

Limitations

Limitations are defects, shortcomings, or potential problems that could affect the research and limit the scope of the findings in the research (Kirkwood & Price, 2013). A potential limitation to this study was that it involved a pretest, training, and posttest. There was a possibility that some participants of the study could have dropped out during the study for various reasons including lack of interest in the study. To counteract this limitation, I computed a minimum sample size, then identified a sample size that accounted for attrition (a larger pool of participants for the pretest, training, posttest if participants dropped out, failed to complete, or submitted invalid tests). There was also a challenge of ensuring participants in either group did not access any formal or informal training immediately prior to the training intervention, or ensuring that the control group did not receive any training, as this would have presented a biased outcome.

Significance of the Study

The public sector of the Commonwealth of Dominica has invested significantly in resources necessary to support its information systems. Some of the perceived benefits of this investment included providing a platform for conducting eCommerce and making government services available and accessible anywhere, anytime, thereby reducing the cost of doing business. Governments all over the world are suffering major financial losses because of cybersecurity threats (O'Driscoll, 2018). It is important that the public sector of the Commonwealth of Dominica protect its information systems investment from threats and vulnerabilities because of cybersecurity. My research was important as it quantified the extent to which employees within the public sector of the Commonwealth of Dominica were aware of cybersecurity and if that awareness could have been improved through training.

My study may provide the public sector of the Commonwealth of Dominica a baseline understanding of the level of awareness that currently exists. In addition, my research assessed the extent to which training impacted the level of employee knowledge of cybersecurity threats which could ultimately reduce the volume of cyberthreats.

Significance to Practice

It is important for users including managers to understand cybersecurity to create policies to support advances in the use of technologies within the organization. The results of the experimental study can form the basis of a framework for further training of all users of information technology including information technology practitioners. Natarajan and Edwards (2016) stated that cyberattacks are evolving and so it is important to know the awareness of the users in the organization of cybersecurity threats and whether those users can counter the evolving cyberattacks.

Significance to Social Change

My research can lead to positive social change by providing the public sector of the Commonwealth of Dominica with a more objective understanding of the current level of awareness of cybersecurity which in turn can promote better training and a more responsible use of the internet. The insights gained can be used to promote the use of eGovernment more effectively to citizens of the Commonwealth of Dominica and build user confidence by enabling them to access the online services in a safe and secure manner.

Summary and Transition

A growing concern for the public sector of the Commonwealth of Dominica is cybercrimes. The headlines of cybercrimes have further heightened these concerns. Further, a lack of awareness about cyberthreats is a severe and unending problem to the management of information security within the public sector of the Commonwealth of Dominica (NTRC, 2015). Therefore, it has become necessary to take steps to address the cybersecurity concerns to align the awareness of cybersecurity by employees to meet any potential threats.

In this study, I examined the level of employee awareness of cybersecurity within the public sector of the Commonwealth of Dominica. In Chapter 2, the literature review covers the information provided by information technology practitioners and scholars on cybersecurity and cyberthreats. I cover the recommended areas of best practices for the protection of information systems and data.

Chapter 2: Literature Review

The purpose of this quantitative experimental study was to explore the role and effectiveness of employee training focused on user awareness of cyberattacks and cybersecurity, with the intent to close the gap in understanding the level of awareness of cybersecurity within the public sector of the Commonwealth of Dominica. The target population of this experimental study consisted of employees within the public sector of the Commonwealth of Dominica. The social problem was that the lack of awareness of cybersecurity by employees within the public service and government agencies in the Commonwealth of Dominica has created conditions in which cyberattacks are doing harm to the information systems (see Aguinaldo, 2018; Alavi & Leidner, 2001; Skarga-Bandurova et al., 2016).

In an increasingly connected world where the internet, technology and digitally enabled services are becoming an integral part of the public sector, cybersecurity continues to play a critical role (de Bruijn & Janssen, 2017). The growing dependency on information and communication technology highlights the risks associated with the use of information and communication technology (Kim, 2017). The literature review provided the background information on the study by looking at existing published research that examined cybersecurity but focused on employee awareness and training. Chapter 2 is divided into three major sections: the literature search strategy, theoretical foundation, and the literature review.

Literature Search Strategy

The literature review included articles, journals, magazines, conference reports, case studies, and books relating to content on user awareness of cybersecurity, cyberattacks, and training from the public library in the Commonwealth of Dominica, the University of the West Indies Open Campus library, and the Walden University Library website. The terms and keywords used in the search process included *cybersecurity*, *cyberthreats*, *cyberattacks*, *user awareness*, *cybersecurity training*, *knowledge of cybersecurity*, and *social cognitive theory*. Some of the phrases used in the advanced filter focused on *social cognitive theory*, *cybersecurity*, *user awareness of cybersecurity*, and *knowledge of cybersecurity.* The search results produced limited results on cybersecurity in the public sector of the Commonwealth of Dominica. I used public official documents from the government of Dominica that referenced *eGovernment* and contained information from international organizations responsible for cybersecurity in the region.

The databases I used were Google Scholar, EBSCO, Emerald Insight, ACM Digital Library, IIEE Computer Society Digital Library, Science Direct, and ProQuest Central. My search included conference reports, articles, and journals that were published in the last 5 years. I used a Boolean search strategy using the following combinations of keywords: *cybersecurity and user awareness*, *cybersecurity training and cyberattacks*, *quantitative research*, *internet*, and *user knowledge of cybersecurity*.

I used journal-filtering to increase the search results to within the last 5 years; however, emphasis was placed on results within the last 3 years given that the subject matter is constantly evolving. Further, I concentrated on articles in reputable technology journals such as *Communications of the ACM*, *Technology in Society*, *Computers & Security*, *MIS Quarterly*, and the *Journal of the Association for information systems.*

Theoretical Foundation

Social cognitive theory (SCT) is a social learning theory that is used in disciplines such as management and information technology. SCT was developed by Bandura (1977, 1986, 1988, 1989, 1998, 2000, 2001, 2004, 2009) and was founded on a relationship in which cognitive, behavioral patterns, and environmental events are operating as interrelating factors that can impact one another. SCT explains changes in human behavior focusing on the relationship among the behavioral, environmental, and personal factors of employees (Wood & Bandura, 1989). It also explains how human beings within social systems can enact several human processes including acquiring and adopting knowledge and information (Wood & Bandura, 1989). SCT theorists (including Wood and Bandura) have suggested that employees acquire behaviors through external and internal social reinforcement. Rooted in SCT is the belief that human beings incorporate self-organization, self-reflectiveness, and self-regulative mechanism into their decision-making and behavior. SCT provides the framework for understanding the mechanism that influences human thought and behavior (Bandura, 1986).

According to Bandura (2001), the key components of the SCT that can influence the behavior of employees include the following:

- Self-control: monitoring the employees’ behavior as well as regulating the behavior of the individual.

- Expectations: assessing the employees’ behavior change as it relates to the expected outcomes.
- Self-efficacy: this is the belief that an employee can control his behavior and is able to perform that particular behavior.
- Behavioral capability: this is understanding and knowing the skills necessary to for employees to perform a behavior.
- Expectancies: This is the value that is added to the outcomes of the employees’ behavior change.
- Observational learning: This is observing the employees’ outcomes based on the performing certain behaviors.
- Reinforcements: This is rewarding employees for changed behavior.

Two significant components that support and influence human behavior are outcome expectancy and self-efficacy beliefs. Outcome expectancy is the belief that there will likely be consequences when a specific behavior is enacted. It is also seen as an enticement for employees to perform that specific behavior. Employees will usually perform a specific behavior if there is an incentive to do so (Bandura, 2001). Self-efficacy is the belief of an employee that he or she can achieve a particular goal or task in any setting. In SCT, self-efficacy is the concept that relates learning and skills development to the goal or task that the employee can achieve. Bandura (1977) acknowledged that cognitive facilitation of action can motivate and enable the processing of the changes that can occur because of the behavior of employees. Self-efficacy can also contribute to the effectiveness with which employees are able to master behaviors as well as influence how employees are able to apply their skills (Bandura, 1998). In SCT, Bandura (1989) identified self-efficacy as one of the critical factors that drive the behavior of employees and individuals. This is done through motivation, cognitive, and affective intervening processes. Hwang et al. (2017) and Hadlington (2017) suggested that employees who possess a strong self-conviction about their ability to use cognitive resources and can take the course of action necessary to succeed, often possess a high level of self-efficacy.

Prior research on cybersecurity has suggested that the environment and social cognition have influenced the behavior and perspectives of employees as it relates to cybersecurity (see Merhi & Midha, 2012; Moody & Siponen, 2013). Using SCT in that context, the premise is based on the belief of employees as it relates to protecting the information systems and information as well as being able to explain the current cybersecurity practices.

Ferrillo and Singer (2015) defined *security practice* as behavior that is exhibited by the adoption of security technology, and an awareness of security behaviors related to the use of the internet and computers. Cybersecurity theories view some behaviors of employees as having dire consequences on the information systems and data. The importance of the role of employees have been highlighted and underscored (Brown, 2015; Hiller & Russell, 2013; Lai et al., 2012) in addressing cybersecurity system security issues in the organization. For this reason, it is critical to develop employee cybersecurity awareness training programs that are capable of improving the cybersecurity posture as it relates to the public sector of the Commonwealth of Dominica.

In social systems, human adaptation and change are significant components. Human activities are created through the social systems and are organized, guided, and regulated in specific domains authorized by certain rules and regulations. Bandura (2001) believed that human behavior is not fully understood solely in terms of social structural factors. Human behavior is not just reactive but operates proactively and generatively. The research questions in my study asked the level of cybersecurity awareness of employees in the public sector of the Commonwealth of Dominica. Understanding the level of employee cybersecurity awareness and how employees can integrate measures that can prevent cyberthreats and cyberattacks (Hiller & Russell, 2013) can contribute to my current research and expand prior research of SCT to many aspects on the functioning and behavior of employees as it relates to cybersecurity.

Prior research on SCT included the extensive use of its application in applied psychology especially as it relates to learning in various contexts. SCT has been used in formal training; however, recent researchers have explored aligning SCT with other training and educational models. Carillo (2010) reviewed the use of SCT in the field of information systems with a focus on understanding the behavior of employees in the adoption and use of technology. Further, Carillo emphasized the relationship between social and cognitive factors that considers learning as a determining factor in changed behaviors. Case and Given (2016) and Pálsdóttir (2013) contended in their studies of knowledge-sharing that the research on SCT had mainly focused on learning in an online environment where the emphasis was on identifying factors that can motivate employees. While reviewing the literature, I found no research that refutes the central concept of

Bandura’s (2001) SCT that pertains to an employee’s ability to perform a behavior through knowledge and skills (as described by Gonçalves de Lima et al., 2020).

In considering existing theoretical frameworks for this study, the existing research has demonstrated that SCT is a valuable tool in studies that focus on learning, and knowledge-sharing. Further, SCT is successful in the development of a framework that supports the changed behavior of employees through learning in the workplace. I used Bandura’s (1977) SCT as the theoretical foundation for this study because it explained the behavior of employees related to safeguarding information systems from cyberthreats and cyberattacks. More specifically, the use of SCT in my study was valuable in filling the gaps in knowledge relating to user awareness and knowledge of cybersecurity.

Literature Review

Information Security

Prior research has revealed that traditionally, a technological approach had been used to protect the information and information assets from any potential cyberthreat or cyberattack (see, Carcary et al., 2016). Using technical tools can be considered essential in the protection of information and information assets. However, in response to the research of Carcary et al. (2016), organizations including governments have looked for ways to be pre-emptive in protecting the information and information systems from human actions. Antoniou (2018) summarized that just using a technology tool is not adequate in fighting certain human actions such as sharing a password with other employees or accessing confidential documents on an open WiFi connection. Other researchers who have suggested that attention should not only be drawn to the technical issues but to the employees as a potential cybersecurity risk include Maynard et al. (2018). They suggested that an employee can be considered as a main factor that contributes to the attacks on information and information systems by cyberthreats. Similarly, McLane (2018) revealed that there is a need to secure the information and information assets from the employees who are considered predominantly the weakest link.

Another factor that influences information security is knowledge. For example, Kim et al. (2014) used a quantitative study approach to explore the factors that prevent employees from complying with security procedures that could prevent cyberattacks. They found that lack of knowledge hinders the use of preventive measures in the adoption of information security. This is similar to research conducted by Alqahtani (2017) who found that employees believe that knowing how to identify cyberthreats is a primary factor in the adoption of information security prevention measures.

The increase in the use of network solutions has resulted in an increase of threats and vulnerabilities to information systems (Adebayo, 2012; Chul et al., 2016; Ferrillo & Singer, 2015). Ferrillo and Singer (2015) concluded that the risky behaviors of employees could have a negative effect on the information and data systems. The perception of employees as it relates to risk is closely related to the behavior choices of the employees (Ahmad et al., 2019; Ferrillo & Singer, 2015). Dang-Pham et al. (2017) argued that the behavior choices of employees could have implications for the management of information systems. This was supported by Hadlington (2017) who looked at the characteristics and beliefs including issues relating to the public sector and how this has impacted the behavioral intentions of the employees on information and cybersecurity. Further, the actions and attitudes of employees in dealing with security issues of information systems was examined by Gordon et al. (2015) and Hwang et al. (2017) and revealed that employees can develop a sense of right and wrong where cybersecurity is concerned.

Fietkiewicz et al. (2017) described information security as the general theme and foundational platform for the development of any cybersecurity awareness program. The responsibility of protecting information within the government is not only the business of managers and supervisors but also of all employees (Gordon et al., 2015). Dykstra and Spafford (2018) shared that the study of the human impact on information security is necessary to provide a foundation to enhance cybersecurity tools as well as to give employees a cybersecurity awareness program that can counter any cybersecurity threats faced.

The globalization of communication between information systems networks has made it possible to steal or guess the identifications and access of information systems (Gabriel & Mohamed, 2011; Solari, 2012). Further, with the globalization of the information systems networks, it is a challenge to know the locations cyberthreats because most cyberthreats or cyberattacks are not physically located where the attack is taking place (Gabriel & Mohamed, 2011). However, Bland et al. (2020) developed an algorithm to identify script comments and malware tactics to track the origins of cyberattacks to prevent hacks and mitigate cyberattacks. Conversely, Solari (2012) reinforced the original view by looking back at the factors that contributed to cyberattacks and summarized that there was a need to focus the mitigation of threats to information and information security by identifying factors that can promote behaviors in employees that will raise the awareness of cybersecurity.

Internal Threats

Internal threats include employees, contractors, and managers who have been trusted with access to the information and information systems. Some researchers (e.g., Ahmad et al., 2014; Glasser & Taneja, 2017) have focused on internal threats where the intention was malicious, and the intention was planned. Theft of information for financial gain and revenge are internal threats that fall into the category of malicious internal threat that was planned. Ahmad et al. (2015) identified internal threats and why the threats have a negative impact on information security. Other researchers (e.g., Harnett, 2016; Kshetri, 2013) have focused on those employees who are internal threats but do not have any malicious intent. Simply the employees are not able to manage the information security within the organization. Harnett (2016) described internal threats as the threats that originate from within the organization. In evaluating the literature on internal threats, Ahmad et al. concluded that the common theme of lack of cybersecurity awareness and unacceptable employee behavior were major causes of internal security incidents and serious threats to information security. According to Gabriel and Mohamed (2011), internal threats can be reduced or mitigated by understanding how or what influences the behavior of employees. Notwithstanding this, Kshetri (2013) stated that regardless of the factors that influence the cybersecurity behavior of employees, it is important for employees to have the knowledge and skills to be able to comply with information security policies, processes, and procedures.

External Threats

These threats include past employees, hackers, natural disasters, and other government agencies. External threats do not have privileges or access to the information systems (Harnett, 2016). In research on cybercrimes, Stephen (2011) reported that a major external cyberattack was the Denial of Service (DoS) attacks on Estonia in 2007. This was a notable and benchmark attack because it affected the entire country over a period of 22 days and every digital service including telecommunication providers, media outlets, and most of the general public were affected. The malicious traffic of the cyberattacks all originated outside of Estonia.

Understanding the influences on user awareness and knowledge of cybersecurity is a relevant problem for several reasons. First, scholarly research (see Asllani et al., 2013; Ki-Aries & Faily, 2017; Knapp & Ferrante, 2012) has indicated that user awareness of cybersecurity contributes to the general decrease in cyberattacks on information systems. By not adopting a cybersecurity awareness posture, the organization loses an opportunity to prevent cyberthreats and to implement information security policies and procedures (Ki-Aries & Faily, 2017). For instance, Hajli and Lin (2016) found that developing information security policies, employees were able to integrate the policies in their day-to-day activities such as not using an open WiFi to access the files of the organizations or sharing the password to their computer with other colleagues.

Among the research contributions that focused on the organization's poor information systems maintenance and management as a factor in cyberattacks rather than the employees, the case study by De Bruijn and Janssen (2017) revealed the role of the organization in the prevention of cyberattacks. The researchers suggested that information security breaches and cyberattacks requires good governance and refocusing on information security management. Steinbart et al. (2016) conducted an extensive literature review on cybersecurity trends and to look at possible solutions against cyberattacks. They concluded that many organizations failed in securing their information systems against cyberthreats and cyberattacks thus creating vulnerabilities and backdoors for hackers and other illegal access. In addition to this, Steinbart et al. suggested that organizations should invest time and money to train end-users, and establish security policies and procedures. Creasey (2013) asserted that this is critical but often overlooked because a lack of awareness or resources in the organization.

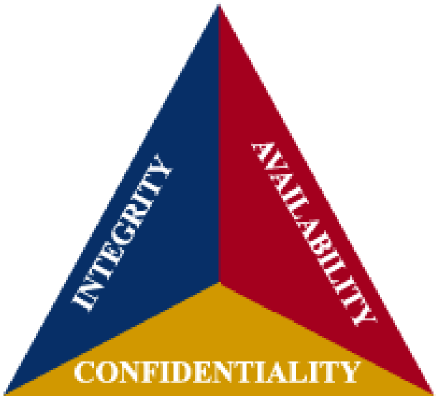
Contextual Influence of Cybersecurity

In reviewing the context of cybersecurity, researchers (for example, Nam, 2019; Mueller, 2017) have looked at cybersecurity-related concepts as important components in understanding how to close the knowledge gap on user awareness of cybersecurity. This is critical in understanding the research problem in my study which was the lack of knowledge and understanding of the level of awareness of cybersecurity and the role and effectiveness of employee training to enhance cybersecurity. In exploring the literature review, there are many similarities between the related concepts such as cyberattacks, cyberterrorism, and cyberwarfare (Nam) and thus it is often difficult to distinguish between them. Notwithstanding the similarities of the concepts, the confidentiality, integrity, and availability of information systems are attacked using the same approaches. Hwang et al. (2017) concluded that employees' lack of awareness and knowledge of cybersecurity can be considered detrimental to the confidentiality, availability, and integrity of any information systems is critical to developing cybersecurity awareness programmes.

The Confidentiality, Integrity, and Availability (CIA) triad is a model (Figure 1) that depicts the main goals to achieve security of information and information systems (Glasser & Taneja, 2017). The focus of the goals of the triad is the protection of information and information systems. Glasser and Taneja mentioned that there are various factors that can determine the security of information systems. However, the focus has been on the three most significant factors, namely confidentiality, integrity, and availability that makes up the CIA triad. The prolific use of information systems and related technological assets in the everyday life warrants the need to develop, and implement mechanisms for protecting information and information systems against cyberthreats and cyberattacks (Halabi & Bellaiche, 2018).

Figure 1

CIA Triad



Note. This figure depicts a model that was designed to guide the development of information security policy. From “Exploring the New Era of Cybersecurity Governance” by Eugen, P. & Petruţ, D., 2018, *Ovidius University Annals: Economic Sciences Series XVIII*(1), 358–363.

Confidentiality Model

In contrast to availability and integrity, confidentiality is the security principle that is used to control the access to information (Halabi & Bellaiche, 2018). The confidentiality model uses measures to ensure that sensitive information or data does not reach the wrong individuals. Access is restricted to employees who are authorized to access the information. Information or data is categorized according to the access level in the event and that the information or data is accessed by the wrong person (Kumar & Kaur, 2014). Researchers (for example, Glasser & Taneja, 2017; Halabi & Bellaiche, 2018) have agreed that in order to protect the confidentiality of the information, employees may require special training to familiarize themselves with the security risk factors as well as to teach employees how to guard the vulnerable information assets. Halabi and Bellaiche stated that confidentiality is similar to integrity, and availability in that the three factors are focused on the prevention of unauthorized access to information systems. In addition to this, all three factors promote using similar methods to include strong passwords in mitigating against cybersecurity and cyberthreats.

Integrity Model

Unlike the confidentiality model that deals with the security principle that is used to control access to information, the integrity model protects the system data from changes that are either intentional or accidental (Warkentin & Orgeron, 2020). The integrity model is primarily concerned with maintaining three goals that include preventing unauthorized users from modifying the data or programs, preventing authorized users from making changes that are not in keeping with required modifications, and maintaining internal and external reliability of the data and the programs (Kumar & Kaur, 2014). In contrast to confidentiality and availability, integrity focuses on the consistency, accuracy, and trustworthiness of the data (Warkentin & Orgeron, 2020). This is important in that cyber threats are often interesting in sensitive data from government in order to sell to competing governments or to use the data against the government. By maintaining the consistency or accuracy of the data, the government can recognize any breach or any unintentional changes or deletions from unauthorized users and even employees. The integrity model stresses the need for backups and redundancy plans to provide for flexibility in restoring data in the event of a cyberattack.

Availability Model

In the availability model, the data and resources are made available for authorized use mainly during disasters and emergencies (Zak & Ware, 2020). As it relates to the availability models, there are challenges that employees are faced with to include Denial of Service (DoS) attacks. This is a program written for the purpose of causing intentional attacks or more specifically, crashes the network when implemented. The availability model identified another challenge in the loss of information system as a result of natural disasters and the actions of human. The guideline in ensuring that reliable access to sensitive data by authorized employees is detailed in the availability model. The availability model also provides a guide to government in how to maintain the hardware and software that is needed to protect itself from cyberattacks.

Cybersecurity Awareness

Parsons et al. (2014) revealed that a growing problem with many governments is how to deal with cybersecurity awareness given that there is a growing dependency on the use of information technology and Information System for daily operations. In order for governments to remain current, there is the need to protect the information assets and to do so, governments must develop and deploy cybersecurity awareness programs that are effective and practical (Maassen, 2018; Aytes & Connolly, 2004).

Montesdioca and Maçada (2015) described cybersecurity awareness as internal programs including education and training that makes employees aware of the practices and policies that governs cybersecurity. Skarga-Bandurova et al. (2016) is of the view that governments are faced with poor cybersecurity awareness as a result of the attitude of its employees. Mohamad Rashid et al. (2013) acknowledged that poor cybersecurity awareness and vulnerabilities can be attributed to the lack of knowledge of cybersecurity exhibited by the employees. Udroiu (2018) cited training and education as being major factors in raising the cybersecurity awareness of employees within public sector. On the other hand, Nasir et al. (2017); Mohamad Rashid et al. believed that while most public sectors have developed security policies to protect the information assets, having security policies and standards can only be fully implemented and adhered to if the employees are aware of the policies and are able to comply with those policies and standards.

Gascó (2017) stated that the implementation of security training programs by governments is an attempt to diminish security breaches and concerns. However, Tang et al. (2016) discussed the results of security training programs as not always being successful because employees often reverted back to the practices that were insecure such as accessing peer to peer websites or providing passwords to unknown individuals who requested the information through spam emails. Nasir et al. (2017) found that employees who were not aware of the risks associated with cybersecurity, often did not see the need to follow such policies. Nevmerzhitskaya et al. (2019) reminded that keeping cybersecurity updated, and improving the awareness and resilience with responsive practices is another way of defending both known and unknown cyberthreats. ESET (2018) conducted a cybersecurity study which revealed that one third of the participants of the cybersecurity study had no cybersecurity training. The study also revealed that 16% of the participants were not aware of any cybersecurity training that was being conducted. Further, participants of the cybersecurity study expressed a willingness to attend the cybersecurity training if offered.

Economic Influence on Cybersecurity

Governments have often highlighted the high cost related to cyberattacks and the management of vulnerabilities that do exist and the impact on its information systems and networks (Flores et al., 2014). In the Caribbean region, the private sector has increased its spending on cybersecurity prevention methods, whereas, the public sector has focused its investments into other priority areas, such as the building of roads, and have not invested any significant resources towards mitigating or combating cybercrimes (OAS, 2016). In its Global Cybersecurity Index, the International Telecommunication Union (2019) asserted that a cyberattack can force the public sector to deviate from other disasters to respond and recovery from a cyberattack. The first cyberattack was in 2017 when the Lands and Surveys Division data server in the public sector of the Commonwealth of Dominica was attacked by a ransomware. The Technical Services Division had invested over $500,000 in collecting geo-spatial information on the location of private and public lands and had redrawn the existing government buildings and other buildings of significant importance to the Commonwealth of Dominica. This caused a significant impact on the work of the Technical Services Division since all the drawings needed for work continuation were erased. The second cyberattack occurred in 2018 on the online payment website of the Inland Revenue Division of the government of Dominica which had a significant impact on the government’s revenue as a result of users not being able to file their tax payments.

Chen and Dongre (2014) discussed the recovery cost and economic damages from a cyberattack. Cyberattacks include not only the theft of confidential data and information but the lost productivity, the disruption of the normal courses of business operations, and loss of reputation. The Herjavec Group (2020) in its annual report stated that cybercrime will cost the global economy in excess of $6 trillion annually by 2021.

The publication of the economic fallout of cyberattacks and information breaches can be another way to raise awareness of employees to the potential risks and damages of a cybercrime (Chen & Dongre, 2014; Clinton, 2015). Weishaupl et al. (2018) conducted a case study that focused on the estimated costs of the lost hours of work of employees who were involved in the cyberattacks and those who had to manage the results of the exploitations of the cyberattacks and data breaches. In the public sector of the Commonwealth of Dominica, the loss of reputation may hinder the adoption of digital services by citizens thus reducing the government's ability to realized future saving through any digital services.

Sources of Cyber-Attacks

The National Institute of Standards and Technology (NIST) provided a list of the various threats to cybersecurity in its publication of NIST 800-82 which is a guide to Supervisory Control and Data Acquisition (SCADA) (https://www.serdp-estcp.org/). This include the following threats:

Hackers

Grimes (2017) described hackers as individuals who exploit the weaknesses in a computer of another individual or gain access into a network without permission in order to steal, destroy or change the information on the computer. Hackers are usually computer programmers who are knowledgeable about computer security. Malwares are installed without the knowledge or consent of the person. Hackers are also able to download attack scripts and protocols from the internet and use them against the websites of the victims. Hackers are classified based on the intent of their actions.

Bot-Network Operators

A botnet is a collection of devices that are connected to the internet and have been infected with a bot program thus providing access to an attacker who is able to take control over them (Grimes, 2017). The hackers are known for taking over multiple systems so that a coordinated attack can be done with the purpose of distribute phishing schemes, spam, and malware attacks. The information collected are then sold in underground markets. Desktop computers are the most common type of device that are targeted for botnet attacks.

Criminal Groups

The attacks on systems are often done for monetary gains by criminal groups using spam, phishing, and spyware/malware in order to commit identity theft or online fraud (Grimes, 2017). The goal of criminal groups is general based on profits but the group is known to attack the infrastructure of governments. The criminal groups are also capably of hiring or developing hackers.

Insiders

The insider is generally a disgruntled person who is the principal source of the computer crime. The insider does not need a great of knowledge about computer intrusions but rather adequate information to cause damage to the information system or to steal data from the organization (Grimes, 2017).

Phishers

Phishers are small groups who carry out phishing schemes to steal identities or information for financial gains (Grimes, 2017). Phishers also uses spyware and or malware on information systems as a means of gaining access.

Spammers

Spammers are individuals who distribute unsolicited e-mail that contains false information so as to sell products, and distribute malware or spyware in order to attack the organization including causing a denial of service (Grimes, 2017).

Spyware/Malware Authors

Spyware or malware authors are individuals or organizations with malicious intent of carrying out attacks against users by creating and distributing the spyware or the malware. Over the years, several computer worms and viruses have destroyed files and hard drives of many organizations (Grimes, 2017).

Cybersecurity Security Awareness

Taitto et al. (2018) maintained that cybersecurity is more about employee’s behavior than it is about anything else. It is the intentional and unintentional actions of employees that causes adverse consequences for which it is necessary to employ security preventive measures. Aldawood and Skinner (2019) stated that while security vendors are hyped about the security products and the need for security products, there are technologies and activities that cannot be automated. For example, Aldawood and Skinner shared that the successful use of the technology is dependent on the implementation and operation of the technologies by people and therefore, the public sector is dependent on people for the achievement of an environment that is secured from cyberattacks.

Istikoma et al. (2015) and Ifinedo (2014) discussed cybersecurity awareness as what the employees know or understand as it applies to the information assets and systems. This dovetailed with the argument by Hu et al. (2012) and Hua and Bapna (2013) that employees are the weakest link in most information security breaches. Hua and Bapna described the breaches as results of the failures of employees to follow the guidelines in securing the assets and information systems. Further, Posey et al. (2015) stated that human cybersecurity awareness requires that individuals who are working with information systems needs more time and resources to fully understand the various risks associated with cybersecurity. Chen (2017), Adebayo (2012), and Bauer and Bernroider (2017) stated that the threats of cybersecurity have been identified as an outcome of the need for cybersecurity security awareness which in itself is hard to monitor and control. This can be further explained by the interrelated, interoperability of information systems and the reliant on computer networks by the public sector in providing services and products (Oravec, 2017; Gonzalez-Granadillo et al., 2018). As a result of all of this, cyberattacks have become an escalating threat to the security of not just the public sector but all organizations.

Wallden and Kashefi (2019) examined case studies to discuss the prevention of cybersecurity. de Bruijn, and Janssen (2017) stated that cybercrime cannot be prevented but it can be deterred through cybersecurity awareness. de Bruijn and Janssen also reflected that most cybersecurity prevention focused on dealing with the incident after the fact. The prevention and the investments in cybersecurity often trail behind after the cyberattack had occurred.

Previous research has shown that there are several factors that influence the cybersecurity behavior of employees. Many of the factors include cybersecurity awareness (Gascó, 2017), apparent threat (Henninger, 2017), and perceived vulnerability (Nevmerzhitskaya et al., 2019). Bulgurcu et al. (2010) viewed the initiatives that are designed to increase user awareness of cybersecurity from several dimensions to include comprehensive information about the general guidelines of basic education on security risks, and consequences of cybersecurity threats. Bulgurcu et al. concluded that a major component of cybersecurity awareness is related to cybersecurity training. This included an employee being aware that there were training programs available to educate employees on acceptable safe and secure ways of using the computer and associated risks involved in misusing the computers (Cefaratti et al., 2011). Abraham (2011) and Nevmerzhitskaya et al. proposed that as non-technical measures for the prevention of cybersecurity breaches by employees, cybersecurity education, training and awareness programs must be considered.

Many of the security breaches that are prevalent in organizations have been attributed to the errors made by humans (Webb et al., 2014). Organizations have found it necessary to increase the security awareness of their employees and their knowledge of how to engage in activities and behaviors that are safe from cyberthreats (Wilding, 2016). For example, Webb et al. (2014); VonSolms and VanNiekerk (2013); and Manworren et al. (2016) attributed many social and psychological factors to the behavior of employees in relation to cybersecurity. Anwar et al. (2017) explored the variable of gender to determine the role it played in mediating the factors that could affect the cybersecurity behavior of employees. In their research, Anwar et al. conducted a cross-sectional survey that studied the effect of gender as a moderator variable between psychosocial factors and self-reported cybersecurity behaviors.

Anwar et al. (2017) used an online survey to gather information on the experiences and beliefs of employees in relation to computers and internet security. The 579 participants were pooled from businesses and universities with 481 of the participants being employed full time or part time. Anwar et al. also included the following constructs: perceived vulnerability (PV), peer behavior (PBEH), self-reported cybersecurity behavior (SRCB), computer skills (CS), Internet skills (IS), and self-efficacy (SSE). Thus, Anwar et al. were able to investigate the differences between male and female to the stated constructs and the effect on the cybersecurity behavior of employees. Anwar et al. considered that a higher mean values for perception construct represented a higher perception level. Using a chi-squared test, Anwar et al. found that there was no significant difference in the proportion of men and women at each age category, X^2 (4, n = 481) = 5.41, p = .248. In assessing the effect of gender as a moderator variable, the results of the study showed that gender had some effect on the security self-efficacy (r = -.435, p < .001), prior experience (r = -.235, p < .001) and computer skills (r = -.198, p < .001). The results further showed that gender had little effect on self-reported cybersecurity behaviors (r = -.152, p < .001). Anwar et al. found that men had slightly higher self-reported cybersecurity behavior (mean 5.61, SD 0.86) than women (mean 5.31, SD 0.93).

Anwar et al.'s research (2017) differs from previous studies by Tsai et al. (2016) and Webb et al. (2014) in that it revealed that women were more concerned about vulnerability than men and, therefore, were more likely to conform with security policies than men. Alcaraz and Zeadally (2015) and Conteh and Schmick (2016) also concluded that women were driven by controlled behavior and that men were able to influence the attitude of others towards using technology more than women were able to do. Conteh and Schmick asserted that for cybersecurity training to be beneficial, there is a need to be aware of, and understand the implication of the variable gender on cyber threats so as to best develop cybersecurity program.

Cybersecurity Awareness Training

Tsai et al. (2016) defended the prominence of the human element in cybersecurity. Tsai et al. looked at two approaches to the research activities on this topic. The first approach looked at security awareness to mean employees being attracted to information technology security issues. The second approach (Arora, 2019) looked at employees’ understanding of information technology security and adherence to security policies.

Dekker (2017) discussed the risks associated with information system and the impact of training on employees being aware of cybersecurity and how to mitigate against the dangers that can affect the information systems. Dekker concluded that the cybersecurity awareness and training program encouraged employees to adopt to security behaviors in order to ensure the protection of the information systems and assets. Further, Valiente (2017) suggested that a cybersecurity awareness program is often preempted by a major reported cyberattack and suggested that the training programs were likely to fail unless the employees’ environment and specific cybersecurity challenges were addressed.

Senthilkumar and Easwaramoorthy (2017) found that cybersecurity awareness can be developed by increasing the cybersecurity awareness of employees through workshops and collaboration. Paek and Nalla (2015) performed a phishing campaign and discovered that the employees scored higher on the evaluation after participating in the awareness program. Further, Paek and Nalla concluded that the awareness program influenced the employees into improving their cybersecurity posture.

Rahim et al. (2015) also supported that if employees were not aware of the value of a cybersecurity awareness program, then employees were not able to detect any cybersecurity issue. In addition to this, the employees are also not aware of the risks that are associated with their actions. According to Lai et al. (2012), this can be attributed to the need for an increase in employee cyber training and awareness to avoid unavoidable and accidental mistakes. Lee et al. (2015) further stated that prevention is effective when there are realistic expectations that the punishment or sanctions can be applied.

Measuring the effectiveness of a cybersecurity awareness training program is vital. Adams and Makramalla (2015) provided the general framework for effectively conducting a cybersecurity awareness training program. Along with assessing the behaviors and attitudes of employees, the ability to crack passwords, tracking of who had exploited the information systems, and monthly follow ups were listed as preventative measures for employees. Although this approach was supported by other scholars (Maria et al., 2019; Kim, 2017; Vitunskaite et al., 2019), still many scholars (Wasserman & Migdal, 2019); Boss et al., 2015) believed that a more scientific approach was needed since the informal measures were not considered an effective measurement of cybersecurity. McLane (2018) concentrated on the importance of cybersecurity awareness initiatives. For example, Johnson and Warkentin (2010) deployed a cybersecurity awareness campaign for 50 employees at a government agency. Johnson and Warkentin did not use any metrics and found that it was difficult to measure the effectiveness of a cybersecurity awareness training.

Miranda (2018) alluded that governments had experienced a cyberattack because of its open access to employees and the information that is provided to the general public. In that regard, Soomro et al. (2015) discussed the need to have a balance between providing access to information sharing to the public and ensuring that the information systems are not susceptible to cyberattacks. Soomro et al. summarized that the behavior of employees as it relates to the way in which employees viewed their work can result in either positive or negative cybersecurity implications. Therefore, it is important to have cybersecurity awareness, training, and education for employees so as to minimize the risk that could be caused by cyberattacks (Soomro et al., 2015).

Cybersecurity Awareness Methodologies

Two general methodologies to the study of cybersecurity awareness of employees have been identified by the SANS Institute. The first methodology focused on the assessment of the cybersecurity program that is currently being used and the level of current awareness of cybersecurity in the organization (SANS 2019). The second methodology looked at the effect of any awareness training that focused on the behavior of the employees being trained. While both methodologies considered the importance of the implementation of a training program, there is no agreement as to which methodology delivered the most benefit to the organization. Ferrillo and Singer (2015) discussed the use of surveys with its own weighted criteria to measure the cybersecurity awareness and behavior of employee. Arquilla and Guzdial (2017) proposed a standardized questionnaire focusing on cybersecurity awareness and behavior of employees as the most appropriate measure.

Khalid et al. (2018) used a survey research design that involved 142 second year students who were enrolled in an Innovation and Technology Training Course with Cyber Security as a subcomponent. The objective of the training was to give the students an exposure to the elements of cybersecurity as well as to create an awareness among the students on the online risks associated with cybersecurity and the need to protect themselves. The questionnaire consisted of 6 sections that covered the demography of the respondents, and self-protection. The respondents were also asked to indicate their agreement or disagreement based on a five-point likert-type scale. Khalid et al. calculated Cronbach's alpha (the measure of internal consistency) to test the reliability of the items.

Khalid et al. (2018) noted that the cybersecurity training contributed to the individual's cybersecurity awareness. The study used an all-encompassing survey that was designed to assess the participants' awareness before and after the intervention. Although, the results were not decisive, the study provided direction on the application of surveys to assess the cybersecurity awareness of the participants. Further, surveys have been the primary instrument used in several studies to assess the level of cybersecurity awareness in participants. The study is important in that it concluded that the level of awareness of cybersecurity was impacted by the training intervention received by the participants. This study supported the research question 3: Does a training intervention impact the level of knowledge and use of cybersecurity?

In contrast with Aldawood and Skinner (2019), Khalid et al. (2018) noted the effect that the knowledge of cybersecurity had on the participants' ability to be aware of online risks during the use of the internet. Khalid et al. considered the interplay between the participants influencing cybersecurity awareness in the organization and the organization adopting cybersecurity awareness programs as a result of the training intervention. On the other hand, Aldawood and Skinner noted that organization interpretation of cybersecurity awareness was rooted in the implementation of policies and strategies that employees must follow to migitate against cybersecurity risks.

Aldawood and Skinner (2019) used a qualitative method to conduct the analysis of the challenges and pitfalls that have affected organizations in developing training and awareness programs pertaining to cybersecurity. The purpose of Aldawood and Skinner study was to explore an awareness program developed for training humans on how to protect the information systems of the organization against cyber threats. Aldawood and Skinner also addressed the threats from a hardware concern rather than the employee as a threat to the security of the information systems.

To understand how cybercriminals were able to successfully infiltrate government computers with phishing emails, as well as attack computer and information systems, and steal valuable information, McCrohan, Engel, and Harvey (2010) explored the arrays of available technologies that cyberattacks have been able to use to infiltrate the networks of governments and the responses of users in preventing cybercriminals from invading the networks. Further, the purpose of the research was to look at the impact of cyber threat education and awareness intervention on the security behavior of users.

The methodology employed by McCrohan et al. (2010) was a quantitative analysis of a pre- and post-treatment design of a single, between subjects factor. The research was conducted with 180 subjects in a low-information treatment and 216 subjects in a high-information treatment study for a two-week period. The theory underpinning this study was that individuals perceived security threats as something that they were able to control and therefore they were more than willing to strengthen their security efforts in order to control the security threats. The result of the research was that if individuals were informed of the threats that they were faced with as a result of their online activities and were knowledgeable of their ability to mitigate against security threats, then they would have been more inclined to protect the technologies that provided access to cybercriminals.

Abawajy (2014) explored the various security awareness delivery methods used in the improvement of employees and end users' awareness of cybersecurity and to determine which of the cybersecurity awareness delivery was most successful and preferred by employees and users. While the literature review supported the need to increase employee awareness of cybersecurity, the research was limited regarding the most effective cybersecurity awareness delivery method for that purpose.

Abawajy (2014) used a qualitative exploratory study that sought to provide new information on the subject of the appropriate cybersecurity awareness training delivery method by comparing three different delivery models through experiments. In an exploratory study, Abawajy assessed how effective each delivery method of cybersecurity awareness training is influencing the learning of cybersecurity awareness concepts and skills by employees and users. A small sample size was used since the study was qualitative. The participants completed a questionnaire prior to attending the training in each of the delivery method. The study used a phishing attack to communicate the cybersecurity message. Other researchers who conducted similar studies, Zak and Ware (2020) suggested that phishing attacks are most commonly used to exploit employees and users since it can be overlooked both by technical and non-technical employees. Abawajy focused on text-based, game-based and video-based security awareness delivery methods and randomly assigned participants to each of the three sessions and experimental group.

The data was then collected and analyzed after the participants experienced each of the three cybersecurity delivery method. A post experience questionnaire was also given to the participants after each cybersecurity delivery method to determine whether the knowledge of cybersecurity awareness increased after participating in a particular cybersecurity delivery method. Finally, Abawajy concluded that cybersecurity awareness training is powerful in empowering people with the knowledge to identify cybersecurity threats with video presentation and training as the preferred cybersecurity delivery method. Steinbart et al. (2016) argued that in addition to the importance and promotion of cybersecurity awareness training in preventing cybersecurity threats, that it is also necessary to implement other preventative measures such as creating password requirements, formulating security policies, and introducing intrusion detecting elements.

Summary and Conclusions

In the literature review, I evaluated studies done within the last ten years related to cybersecurity, and information security to understand the various factors that influenced employee awareness of cybersecurity. Most of the researchers in the discipline studied extensively the technical methods that can be used in preventing cyberattacks (Steinbart et al., 2016; Topa & Karyda, 2015) and, in many circumstances, they applied their findings and conclusions toward the improvement of user awareness so as to protect the information systems from cyberattacks and the type of activities that can lead to the exposure of data to cybercriminals and cyberattacks. However, few researchers explicitly focused on the impact of training on user awareness and knowledge associated with the prevention of cybersecurity. Additionally, few studies related the social cognitive theory to cybersecurity and the user perception of cybersecurity training as a factor in mitigating against cyberattacks. While the literature on cybersecurity continues to grow and has an impact on the knowledge that is available on cybersecurity, this growth has mainly been focused on the international hemisphere. Thus, within the Caribbean region and the Commonwealth of Dominica, there is a gap in the research studies on user awareness and the lack of knowledge and understanding of the level of awareness of cybersecurity.

There was a consistent theme found during the analyses of the research studies that captured elements that aligned with the factors that cause cyberattacks on information systems. These factors contribute significantly in understanding the targets and objectives of cyberattacks. The studies that I assessed contributed to the use of security controls that can improve cybersecurity but lacked focus on the factors that affect the adoption or implementation of security controls. Understanding the factors is beneficial in the development of cybersecurity user awareness programs and training intervention. Based on the gap in the literature on the lack of user awareness of cybersecurity, I used a quantitative experimental research design which may be useful in adding to the knowledge on cybersecurity. I discuss in Chapter 3 the research methods that focused on employee awareness of cybersecurity and the impact of training in raising awareness of cybersecurity in order to overcome internal human factor as the weakest link in the cybersecurity chain. Chapter 3 also includes a description of the research design, the methodology, and the data collection and data analysis strategies.

Chapter 3: Research Method

The purpose of this quantitative experimental study was to explore the role and effectiveness of employee training focused on user awareness of cyberattacks and cybersecurity, with the intent to close the gap in understanding the level of awareness of cybersecurity within the public sector of the Commonwealth of Dominica. The target population of this experimental study consisted of employees within the public sector of the Commonwealth of Dominica.

Chapter 3 introduces and discusses the research methodology, the research redesign, and rationale. The process of data collection is reviewed, the data analysis plan, and the ethical issues related to the data collection process are documented and clarified.

Research Design and Rationale

I used a pretest, posttest controlled experimental design in this study. The employees participating in the study were divided into a control group and an experimental group. The DV was the score on a test of awareness and knowledge of cybersecurity. The IVs were time (pretest and posttest) and group (control and experimental). The demographic information collected in this study included gender as a categorical variable with two values (male or female), age as a numerical variable (collected as years and months to be converted to decimal continuous), location of the participants with three categories (city, urban, and rural), and access to the internet in the public sector of the Commonwealth of Dominica defined as the number of monthly interruptions.

As stated in Chapter 1, the research question and hypotheses for my study were the following:

RQ1: What is the level of cybersecurity awareness and knowledge in the public sector of the Commonwealth of Dominica?

This research question was intended to establish through descriptive statistics a quantified baseline understanding of the level of cybersecurity awareness. In addition, the following hypotheses were tested to establish a baseline difference between the two groups (control and experimental):

$H_0$1: There is no difference in the level of knowledge and use of cybersecurity between the control and experimental groups during the pretest.

$H_0$1: $\mu_C = \mu_E$ (where μ_C is the mean score for the control group, and μ_E is the mean score for the experimental group)

H_a1: There is a difference in the level of knowledge and use of cybersecurity between the control and experimental groups during the pretest.

H_a1: $\mu_C \neq \mu_E$

RQ2: What is the level of cybersecurity awareness and knowledge according to demographic factors age, gender, location, and access to the internet in the public sector in the public sector of the Commonwealth of Dominica?

$H_0$2: There is no difference in the level of cybersecurity awareness and knowledge according to demographic factors age, gender, location, and access to the internet in the public sector of the Commonwealth of Dominica.

$H_0$2: $\beta_1 = \beta_2 = \ldots = \beta_k = 0$ (all coefficients = 0)

H_a2: There is a difference in the level of cybersecurity awareness and knowledge according to at least one of the demographic factors of age, gender, location, and access to the internet in the public sector of the Commonwealth of Dominica.

H_a2: at least one $\beta_j \neq 0$

RQ3: Does a training intervention impact the level of knowledge and use of cybersecurity?

H_03: The experimental group demonstrates a level of knowledge and use of cybersecurity equal to or lower than the control group as measured during the posttest.

H_03: $\mu_E \leq \mu_C$ (where μ_C is the mean score for the control group, and μ_E is the mean score for the experimental group)

H_a3: The experimental group demonstrates a higher level of knowledge and use of cybersecurity than the control group as measured during the posttest.

H_a3: $\mu_E > \mu_C$

RQ4: Is there a change or increase in the level of knowledge and use of cybersecurity for the experimental group from the pretest to the posttest?

H_04: There is no change or a decrease in the level of knowledge and use of cybersecurity for the experimental group from the pretest to the posttest.

H_04: $\mu_D \leq 0$ (where μ_D is the mean difference of scores for the participants in the experimental group, from pretest to posttest)

H_a4: There is an increase in the level of knowledge and use of cybersecurity for the experimental group from the pretest to the posttest.

H_a4: $\mu_D > 0$

I chose this research design based on the research problem. The research problem was the lack of knowledge and understanding of the level of awareness of cybersecurity and the role and effectiveness of employee training to enhance cybersecurity. I selected the quantitative research design over qualitative and mixed methods designs because the quantitative research method includes the measurements and statistical analysis of data that are collected through a pretest and the posttest (see Frankfort-Nachmias & Leon-Guerrero, 2018). Quantitative research designs perform tests of relationships among measured variables which can explain or predict a phenomenon (Purohit & Singh, 2013). In quantitative research, numerical data are collected and generalized across groups. The qualitative research design was not appropriate to answer the research questions because qualitative research design answers questions about the nature of phenomena with the purpose of understanding the phenomenon from the point of view of the participant (Goldberg & Allen, 2015). My research had the objective of examining the awareness and behaviors of employees and the impact of cybersecurity training which was more suited to a quantitative method.

Methodology

Population

The population for this study was composed of employees who were permanently, temporarily, and contractually appointed in the public sector of the Commonwealth of Dominica. The public sector of the Commonwealth of Dominica is made up of 5,000 employees, both male and female, between the ages of 18 and 60 years.

The target population for this study did not include nonestablished employees. A nonestablished employee is classified as an employee who is paid biweekly. Other employees who were included in the study were interns from the National Employees Programme employed by the public sector but who were assigned to private sector organizations.

Sampling and Sampling Procedures

Frankfort-Nachmias and Leon-Guerrero (2018) described sampling as the process that is used to identify and select the subset of the population for a study. The sampling method used in my study was random sampling. According to Zahid and Shabbir (2018), random sampling allows for generalizing the results of the sample to the target population. I obtained access to the target population with approval from the chief personnel officer.

Stratification was done on gender and age based on the proportion of males (P_m) and females (P_f) within the total population (N_T). The number of males (n_m) and females (n_f) in the sample of n_s was calculated using the formula, $n_m = p_m \times n_s$. While I collected actual age as a numerical variable, for stratification the age distribution was categorized into groups. This grouping considered the fact that the minimum and maximum ages were 18 and 60 respectively, a range of 42 years. Stratification of four groups translates to class intervals of 10.5 years. For simplicity, the groups had ranges of 18 to 30, 31 to 40, 41 to 50, and over 50.

There were two testing groups (control and experimental), two genders, and four age groups; there were a total of $4 \times 2 \times 2 = 16$ bins in the sample. Each member of the population was numbered from one to the population size (N_T). Excel was then used to randomly generate numbers within the interval [1, N_T]. Every selected individual was surveyed and placed in their respective bin until all 16 bins were completed.

Sample Size

I used G*Power software (Faul et al., 2007) to calculate a minimum sample size. The G*Power software, a free statistical power analysis tool, is frequently used in quantitative studies for the purpose of ensuring adequate confidence and power.

The minimum sample size was based on the following assumptions:

- level of significance (α) = 0.05
- statistical power ($1 - \beta$) = 0.90
- medium effect size (.50 for a *t* test, .15 for MLR)
- one-tail hypothesis test
- equal sized groups
- four predictors (for Hypothesis 2: age, gender, location, and access to the internet)

The level of significance (α) is the probability of a Type I statistical error, or false positive—rejecting the null hypothesis when it is true (Mertler & Vannatta, 2013). Statistical power ($1 – \beta$) is the probability that the test will correctly reject a false null hypothesis (Mertler & Vannatta, 2013). β is the probability of a Type II statistical error, or a false negative—failing to reject the null hypothesis when in fact it is false. In my study, the power = 0.90, indicating a 10% probability of failing to reject a false null hypothesis.

The effect size is an indication of the degree in which an occurrence is present in a population or detected by the statistical test used in the study (Cohen, 1988). Cohen (1988) suggested effect size of $d = 0.2$, d = 0.5, and d = 0.8 for small, medium, and large respectively (for *t* tests). Using a significance level of $\alpha = 0.05$, and a statistical power of 0.90, I used a medium effect size of 0.5 for a *t* test, and 0.15 for MLR. This was to provide for an acceptable probability of detecting a difference of means in the DV between the controlled and experimental groups.

The effect size (d), significance level (α) and power ($1 - \beta$) were input into to G*Power to determine the sample size, n_s. For the chosen parameters, the one-tail *t* test of means for two samples with pooled or separate variance required a minimum sample size of 70 per group, or 140 total. A paired *t* test required a minimum sample size of 36. MLR with four predictors requires a minimum sample size of 108. As a result, to ensure each test had the required confidence and power, the minimum sample size was 140, or 70 per group.

Considering attrition due to fallout or invalid tests of 20%, the minimum sample size was 88 per group, or a total of 176, to ensure the desired power and confidence were met. With 16 total bins, or 8 per group, each bin required a minimum of 11 participants. Therefore, I recruited to ensure a minimum of 176 participants; and more specifically, at least 11 participants within each bin.

Procedures for Recruitment, Participation, and Data Collection (Primary Data)

The recruitment process involved contacting the chief personnel officer who is responsible for the management of human resources and employees in the public sector of the Commonwealth of Dominica to obtain the consent in order to recruit participants for the study. Potential participants were contacted via email to request their participation in the study. A consent form was made available to the participants to complete as part of the recruitment process. The purpose of the consent form was to provide information about the study, and details about the collection process which included the training intervention.

The participants met two criteria: they were employed within the public sector as a full-time, part-time, nonestablished or established employee; and they were 18 to 60 years old.

Intervention

By using an intervention, a researcher can examine the impact of a treatment on the participants (Cano-Aguilar, 2020)**.** The control group did not receive the treatment while the experimental group received the treatment. In my study, the intervention was a cybersecurity awareness training program for employees of the public sector in the Commonwealth of Dominica. I used the Security Awareness TrainingPack Courses developed by MediaPro Cybersecurity and Privacy Education. The Security Awareness TrainingPack Courses were purchased from the company for use by the instructors who conducted the training program. The Security Awareness TrainingPack Courses have been taught to over 10 million employees. MediaPro was listed as a leader in the Gartner’s Magic Quadrant for Security Awareness Computer-based Training for over 5 years (MediaPro, 2020).

I took into consideration the technology level of the participants and selected training materials from the Security Awareness TrainingPack Courses that did not require a deep technological understanding. The training materials were in English and addressed data protection fundamentals, insider threats, protecting and handling data, preventing phishing, and security awareness. Two training methods were used during the experimental training for everyone in the experimental group.

Cybersecurity Video Training focused on detecting cyberattacks and provided actionable information on how to detect cyberattacks. The videos were 5 minutes in length and included information on cyberattacks, preventing phishing, and security awareness.

Instructor-led classroom training was scheduled classroom training in a lecture setting with an instructor. The lectures were held 2 days a week for 1 hour and required attendance by each participant. The content created for the instructor-led classroom training were the training materials from the Security Awareness TrainingPack Courses and included data protection fundamentals, insider threats, protecting and handling data, preventing phishing, and security awareness and were similar to the materials in the cybersecurity video training. The lectures were interactive, and participants were encouraged to participate through in-class quiz. Participants were encouraged to ask questions during the lecture and the information was reinforced with examples of cyberattacks and being able to detect any potential attack.

Instrumentation and Operationalization of Constructs

The instrument was an existing risk assessment questionnaire developed by Mediapro as part of the preassessment tool in preparation for the Security Awareness TrainingPack Courses. It was administered as a pretest at the beginning (first day of classes) and as a posttest at the end (last day of classes). With the chief personnel officer’s approval to access the target population, a consent form with the institutional review board (IRB) protocol number was included as part of the data collection instrument.

The instrument had 24 items for the purpose of evaluating cybersecurity knowledge. I modified the instrument to add four questions relating to the demographics of the employee participants which represented the four IVs of age, gender, location, and access to the internet.

The instrument cybersecurity items were in the form of multiple choices and the participants were expected to select the correct response. Each correctly answered question was worth one point. The DV was calculated as the percentage of the correct responses answered out of 24. The DV and IVs are summarized in Table 1.

Table 1

Description of DV and IVs

	Variable	Type	Calculation
DV	Cyber security knowledge	Continuous Numerical	Percentage score from instrument
IVs	Age	Discrete Numerical	Number of years from birth year
	Gender	Nominal Scale	Dichotomous (male/female)
	Place of residence	Nominal Scale	Three Categories
	Internet access	Ordinal Scale	Four-point Likert scale

Data Analysis Plan

The research design was a two-group pretest-posttest design. In a two-group pretest-posttest design, the DV was measured once prior to the implementation of the treatment and then measured once again after the treatment was implemented (Creswell, 2013). The posttest was repeated for both the control group and the experimental group from within the public sector of the Commonwealth of Dominica. Comparisons were made between the groups twice: during the pretest and during the posttest. A comparison was also made for the experimental group between the pretest and the posttest. Hypotheses 1 and 3 were tested using an independent samples *t* test. Hypothesis 2 was evaluated using MLR. Hypothesis 4 was evaluated using a paired *t* test.

Data Analysis Software

I used IBM's Statistics Package for the Social Sciences (SPSS) predictive analytics software version 24. SPSS provides user friendly drop down menus and the ability to analyze large data sets (Mertler & Vannatta, 2013). Most importantly, SPSS is commonly used in quantitative research studies. Microsoft Excel was used in the data analysis.

Descriptive Statistics

Data analysis included descriptive statistics for demographic data and test scores (both pre and posttest). The descriptive statistics included standard deviation, frequency, variance, median, and mean (Warner, 2013). Pie charts graphically represented the gender and location of the participants. Bar graphs provided a visual analysis of the level of internet access and the cybersecurity knowledge and awareness of the participants. The age of the participants was graphically represented via a histogram and a normal distribution plot. Descriptive statistics were used to respond in part to RQ 1 and 2.

Hypothesis Tests

Hypotheses 1 and 3: t Test of Means

The comparison of the means of the pretest scores was in response to the second part of RQ1, to compare as a baseline the two groups prior to the intervention. Hence, if there was a difference in the means of the pretest scores between the experiment and control groups, that difference would have been considered after the intervention. According to Warner (2013), if the experimental group has the greater mean prior to the intervention, it is expected that this superiority will increase after the intervention. However, if the control group displayed superiority in pretest scores, then it was expected that this superiority would have lessen after the intervention. On the other hand, if there was no difference in the means of the pretest scores between the groups, then a simpler case was presented, whereby, both groups were proceeding into the experiment with equal cybersecurity knowledge and awareness.

The comparison of the means of the posttest scores was in response to RQ3, which required a comparison of the two groups' cybersecurity knowledge and awareness after the intervention (treatment applied to the experimental group). A difference in the means of the posttest scores between the two groups after the intervention would have been considered along with the results of the test of $H_0 4$, which compared the pretest and posttest scores of the experimental group. A difference in the means of the posttest scores between the two groups when their pretest scores were equal is evidence of a significant impact made by the intervention on the experimental group. In the case where the group means from the pretest were different, the results of the posttest were analyzed carefully and with the experimental group's change considered.

For the *t* test, I investigated whether the *t* test of mean test scores for the experimental and control groups should be pooled variance or separate variance by first performing the *F* test for equality of variances. The null hypothesis (H_o) was equal variance between the two groups. I rejected H_o if the *p* value < α = .05, and concluded that there was sufficient evidence that the variances are not equal. I then used the separate variance *t* test. If H_0 was not rejected then equal variance was assumed, and the pooled variance *t* test of means for the two groups was used.

For the *t* test of means, whether pooled or separate variance, $H_0$1 stated that the means are equal (for hypothesis 1), and was rejected if the *p* value < $\alpha = 0.05$; in that case, there was sufficient evidence to conclude there is a difference in the pretest score means of the experimental and control groups. On the contrary, if the *p* value > $\alpha = 0.05$, $H_0$1 was not rejected and the conclusion was that there is no difference in the pretest score means of the two groups. This procedure was replicated for $H_0$3 with regards to the posttest scores.

The comparison of the means of the posttest scores (hypothesis 3) was in response to RQ3, which required a comparison of the two groups' cybersecurity knowledge and awareness after the intervention (treatment applied to the experimental group). Similar to hypothesis 1, the *F* test for equality of variance was performed to decide whether pooled or separate variances was utilized. In any case, pooled or separate, if the *p* value < α =

0.05, $H_0$3 was rejected, and there was sufficient evidence to conclude that the mean posttest score of the experimental group was greater than the control group, then that was an indication that the training was effective. However, if the *p* value > α = 0.05, $H_0$3 was not rejected, then there would have been insufficient evidence to conclude that the training is effective.

Hypothesis 2: MLR

$H_0$2 was tested using MLR; the response variable was the level of cybersecurity knowledge and Awareness (*CKA*) among all participants (both groups), while the explanatory variables were gender (*G*), age (*A*), location (*L*), and internet access (*I*). The linear model was of the general form:

$$CKA = b_0 + b_1G + b_2A + b_3L + b_4I + \varepsilon$$

where b_0 is a constant, b_i is the coefficient for the *i*th term, and ε is the error term. An *F* test for the significance of the entire model was performed, as well as a *t* test of the individual IVs. The following was the structure of this test:

Null hypothesis. The hypothesis for the significance of the multiple regression model was there is no linear relationship between the DV *CKA* and the entire set of IVs, which were *G, A*, *L*, and *I*, depicted mathematically as follows:

$$H_0\text{:}\ \ b_1 = b_2 = b_3 = b_4 = 0 \text{ (all coefficients = 0)}$$

Alternative hypothesis. There exists a linear relationship between the DV *CKA* and at least one IV, *G*, *A*, *L*, and *I*.

$$H_A\text{:}\ \ \text{at least one } b_j \neq 0.$$

The null hypothesis is rejected if the p value $< \alpha = 0.05$, indicating sufficient evidence that there is at least one coefficient not equal to zero. If the p value $> \alpha = 0.05$ then H_0 is not rejected, indicating insufficient evidence to conclude that any coefficient is not equal to zero.

The significance of each IV was tested via a *t* test, for which the null hypothesis is that the coefficient, b_j, equals zero. The null hypothesis is rejected if the p value $< \alpha = 0.05$, indicating sufficient evidence that the coefficient is not equal to zero, hence the IV in question is a significant predictor of the DV. If the p value $> \alpha = 0.05$ then H_0 is not rejected, indicating insufficient evidence that the coefficient is not equal to zero, and concluding that this variable is not a significant predictor of the IV. I also computed adjusted R^2 to assess the goodness of fit of the regression model.

Hypothesis 4: Paired t Test

To test H_0, a paired *t* test was applied. The null hypothesis states that the mean difference between pretest score and posttest score is zero or negative (i.e., there is no change or a negative change in group scores following the treatment—no improvement in level of knowledge or a decrease). If the p value $< \alpha = 0.05$, $H_0 4$ is rejected, indicating there is sufficient evidence that the mean difference between pretest and posttest scores is greater than zero (i.e., there is an improvement in scores following the training). Otherwise, the $H_0 4$ is not rejected, and there is insufficient evidence to conclude that the posttest scores are superior than those of the pretest after the training.

Check of Assumptions

For the *t* test, the following assumptions were met:

- Independent and random samples. This assumption was tested using the non-parametric Kruskal–Wallis test.
- Numerical DV with interval or ratio measurement. This assumption was assured during data collection.
- Normally distributed DV. This assumption was tested using the Kolmogorov-Smirnov Test of Normality.
- Population variances were equal. This assumption was tested using the *F* test.

For the paired *t* test, the following assumptions were met:

- Independent and random samples. This assumption was tested using the non-parametric test, Kruskal–Wallis test.
- Numerical DV with interval or ratio measurement. This assumption was assured during data collection.
- Normally distributed DV. This assumption was tested with a normal probability plot of residuals.

For MLR, the following assumptions were met:

- Linear relationship between IV and the DV. This assumption was tested using scatterplots.
- Numerical dependent and IVs. This assumption was assured during data collection.
- No multicollinearity—IVs not correlated with each other. This assumption was tested with variance inflation factors (VIFs).

- Homoscedasticity—variance of the residuals is similar across all values of the IVs. This assumption was tested with the scatterplots of residuals.
- Normally distributed residuals. This assumption was tested with a normal probability plot of residuals.

Warner (2013) stated that in MLR the dependent and IVs must be numerical. Therefore, the categorical variables were converted to dummy variables. Tables 2, 3, and 4 illustrate the conversion of the independent categorical variables gender, location, and access to the internet in the public sector of the Commonwealth of Dominica respectively into dummy variables.

Table 2

Gender Dummy Variable and Coding

Gender	(x_1)
Male	1
Female	0

Table 3

Location Dummy Variable and Coding

Location	(x_2)	(x_3)
City	1	0
Central	0	1
Rural	0	0

Table 4

Internet Access Dummy Variable and Coding

Internet Access	(x_4)	(x_5)	(x_6)
Excellent	1	0	0
Good	0	1	0
Fair	0	0	1
Poor	0	0	0

Threats to Validity

Validity refers to the accuracy, and trustworthy of the concept that is being researched (Warner, 2013). Validity is ensuring that the results of the study are error free, and that the data supports the analysis of the study. Validity is affiliated with quantitative research and developed around casual relationships between the treatment and the outcome of the experimental study.

External Validity

External validity is the degree to which the results of a study can be generalized to another group (Babbie, 2013). The focus of the study was on the lack of user awareness of cybersecurity and the impact of training in the public sector of the Commonwealth of Dominica. The findings of the study were specific to the population in the public sector. Therefore, the results were not generalized to the private sector, and any other country in the Caribbean.

Internal Validity

The extent to which the research design as well as the resulting data will allow for drawing accurate conclusions about the cause and effect of the data is internal validity. Internal validity is also the design of the study and the instrument that is used in the study

(Creswell, 2012). In the research design, there are various types of internal validity that are related to the participants of a study to include history, regression, and selection. History threat involves changes that cannot be controlled during the length of the study (Creswell, 2012). This includes conducting the study for an extended period of time. This influenced the outcome of the study. The study addressed this threat by conducting the study over a four-week period and not longer. Selection can influence the outcome of the study by biasness to the selection of the participants to the study. I used random sampling and thus eliminated the risk of bias. Testing and instrumentation were the two types of internal validity that were related to the procedures of the study. Participants were exposed to a pretest during testing. This can influence the outcome of the posttest. According to Creswell, administering the posttest only once can prevent the threat posed by testing. The change in the measuring instrument that is used between the pretest and the posttest can be considered as an instrumentation threat. Further, Creswell stated that using the instrument in the pretest and posttest by standardizing the procedures can mitigate against this threat. This study used the same measuring instruments in order to avoid the threat of instrumentation.

Ethical Procedures

Approval was sought from IRB of Walden University since the subjects for this study were human beings. After, this, I requested permission from the Chief Personnel Officer of the public sector of the Commonwealth of Dominica. The study was done at no risk to the participants and was done with all ethical considerations in mind. Respect for the participants who were part of the research were of utmost importance in this study. A possible ethical issue addressed was conducting the research within the public sector which is also my place of employment. To ensure that there was no conflict of interest, the participants were protected by voluntarily agreeing to participate in the study. There was no conflict of interest in this study because the participants were participating in the study of their own free will. Participants were not forced in any form to participate in the study and therefore, there were no repercussion if a participant withdrew or declined to participate in the study. There was no risk to the participants given that instructor-led training was not a new concept to the participants. The Government of the Commonwealth of Dominica conducts monthly training that are open to all employees of the public sector. Participants were not offered any incentive to participate in the study and thus addressed the issue of participants receiving an incentive to participate in the study.

Summary

The sections in Chapter 3 included the research method, methodology, population, the sampling and sample procedure, data collection, and data analysis plan. In Chapter 3, I demonstrated an alignment in the research between the problem statement, the purpose statement, and the research questions. My social problem dealt with the lack of awareness of cybersecurity by employees within the public sector of the Commonwealth of Dominica and how this created conditions in which cyberattacks can do harm to the information systems. A quantitative research design was most suitable for this study because of the need to examine the relationship between the variables. In Chapter 4, I will present the results of my study.

Chapter 4: Results

The purpose of this quantitative experimental study was to explore the role and effectiveness of employee training focused on user awareness of cyberattacks and cybersecurity, with the intent to close the gap in understanding about the level of awareness of cybersecurity within the public sector of the Commonwealth of Dominica. The target population of this experimental study consisted of employees within the public sector of the Commonwealth of Dominica. I used a pretest, posttest controlled experimental design in this study. I took into consideration the independent and DVs as part of the MLR to address the following research questions and hypotheses:

RQ1: What is the level of cybersecurity awareness and knowledge in the public sector of the Commonwealth of Dominica?

This research question was intended to establish through descriptive statistics a quantified baseline understanding of the level of cybersecurity awareness. In addition, the following hypotheses were tested to establish a baseline difference between the two groups (control and experimental):

$H_0$1: There is no difference in the level of knowledge and use of cybersecurity between the control and experimental groups during the pretest.

$H_0$1: $\mu_C = \mu_E$ (where μ_C is the mean score for the control group, and μ_E is the mean score for the experimental group)

H_a1: There is a difference in the level of knowledge and use of cybersecurity between the control and experimental groups during the pretest.

H_a1: $\mu_C \neq \mu_E$

RQ2: What is the level of cybersecurity awareness and knowledge according to demographic factors age, gender, location, and access to the internet in the public sector of the Commonwealth of Dominica?

$H_0$2: There is no difference in the level of cybersecurity awareness and knowledge according to demographic factors age, gender, location, and access to the internet in the public sector of the Commonwealth of Dominica.

$H_0$2: $\beta_1 = \beta_2 = \ldots = \beta_k = 0$ (all coefficients = 0)

H_a2: There is a difference in the level of cybersecurity awareness and knowledge according to at least one of the demographic factors of age, gender, location, and access to the internet in the public sector of the Commonwealth of Dominica.

H_a2: at least one $\beta_j \neq 0$

RQ3: Does a training intervention impact the level of knowledge and use of cybersecurity?

$H_0$3: The experimental group demonstrates a level of knowledge and use of cybersecurity equal to or lower than the control group as measured during the posttest.

$H_0$3: $\mu_E \leq \mu_C$ (where μ_C is the mean score for the control group, and μ_E is the mean score for the experimental group)

H_a3: The experimental group demonstrates a higher level of knowledge and use of cybersecurity than the control group as measured during the posttest.

H_a3: $\mu_E > \mu_C$

RQ4: Is there a change or increase in the level of knowledge and use of cybersecurity for the experimental group from the pretest to the posttest?

$H_0$4 There is no change or a decrease in the level of knowledge and use of cybersecurity for the experimental group from the pretest to the posttest.

$H_0$4: $\mu_D \leq 0$ (where μ_D is the mean difference of scores for the participants in the experimental group, from pretest to posttest)

H_a4: There is an increase in the level of knowledge and use of cybersecurity for the experimental group from the pretest to the posttest.

H_a4: $\mu_D > 0$

Chapter 4 covers the data collection procedures, includes a description of the time frame of the data collection, and clarifies any deviation from the planned data collection procedures. Additionally, this chapter covers the results, descriptive statistics, and an analysis of the statistical findings based on the research questions and hypotheses. I conclude Chapter 4 with a summary that answers the research question and the hypotheses.

Data Collection

The sample for this study consisted of employees within the public sector of the Commonwealth of Dominica who were employed as a full-time, part-time, nonestablished, or established employee and aged 18 to 60 years old. I used random sampling with stratification on the two variables of age and gender that allowed for elimination of the risk of bias in the selection process of the participants. The duration of the questionnaire collection period was 3 weeks.

Recruitment

I started the process of recruitment after I received Walden's IRB approval. The IRB Approval Number for this study is 09-25-20-0548049. I contacted the chief personnel officer who is responsible for the management of human resources and employees in the public sector of the Commonwealth of Dominica to obtain the consent in order to recruit participants for the study. On September 30, 2020, potential participants were contacted via email to request their participation in the study. The purpose of the consent form was to provide information about the study, participation criteria, and details about the collection process which included the training intervention. By clicking on the link to the questionnaire, employees of the public sector of the Commonwealth of Dominica agreed to participate in the study. To gather as many responses as possible, on October 22, 2020, I sent a reminder to public officers with the consent form and the link to the questionnaire.

Prior to commencing the research, I assumed that enough employees of the public sector of the Commonwealth of Dominica were interested and available to participate in the training program to meet the calculated minimum sample size. I further assumed that the sample population had the basic computer skills to adequately perform in the training course and that the employees of the public sector in the Commonwealth of Dominica would have participated in testing truthfully and that the data would be reliable. During the conduct of this study, there was no contradiction to these assumptions.

Collection Process

I collected the data using an existing risk assessment questionnaire developed by Mediapro Training Cooperation, modified to include demographic questions (Appendix A). The risk assessment questionnaire was administered online to employees of the public sector of the Commonwealth of Dominica between September 30, 2020 and December 09, 2020. The risk assessment questionnaire required approximately 10 minutes to complete and included 24 questions on cybersecurity for the purpose of collecting information on the cybersecurity knowledge of the employees. The risk assessment questionnaire also included questions relating to the demographics of the employee participants.

Descriptive Statistics for Demographic Characteristics

I estimate that the email invitation for request for participation was sent to over 4,000 employees within the public sector of the Commonwealth of Dominica. I am not aware of the number of employees who read the email request to participate in the study. The request yielded $n = 176$ responses. As a result, the statistical power of $1 - \beta = 0.90$, as outlined in Chapter 3, was met.

The 176 participants met the eligibility requirements. Table 5 summarizes the demographic characteristics of the sample of the 176 respondents.

Considering attrition due to fallout or invalid tests of 20%, the minimum sample size was 88 per group, or a total of 176, to ensure the desired power and confidence were met. With 16 total bins, or 8 per group, each bin required a minimum of 11 participants.

Therefore, I recruited 176 participants and assigned the respondents by dividing into eight bins, each with 11 respondents.

Actual age of the participant was collected as a numerical variable; however, for the purpose of stratification, the age distribution was categorized into groups taking into consideration that the minimum and maximum ages were 18 and 60 respectively. The group ranges were 18 to 30, 31 to 40, 41 to 50, and over 50.

Table 5

Demographic Characteristics of the Sample

Characteristic	*N*	%
Gender		
Male	64	36.4%
Female	112	63.6%
Location		
Rural	64	36.4%
Urban	81	46.0%
City	31	17.6%
Access to the Internet		
Poor	4	2.3%
Fair	24	13.6%
Good	92	52.3%
Excellent	56	31.8%

Treatment Fidelity

Like the rest of the world, the Commonwealth of Dominica was affected by the Coronavirus pandemic which resulted in the country implemented curfew hours and restriction on mass gathering. According to the Ministry of Health, Wellness, and New Health Investment (GIS, 2020), the coronavirus pandemic required social distancing and no mass gathering of any form as measures to contain the spread of the coronavirus. This disrupted the original plan of face-to-face instructor-led classroom training. As a result, the instructor-led classroom training was done online. The content created for the instructor-led classroom training was the Security Awareness TrainingPack Courses and included such topics as data protection fundamentals, insider threats, protecting and handling data, preventing phishing, and security awareness. The lectures were interactive, and participants were encouraged to participate through quizzes and end of week assessments.

The cybersecurity training was conducted for the experimental group for 1 hour, 2 days a week, for 4 weeks from November 05, 2020 to December 07, 2020. The risk assessment questionnaire was given again after the cybersecurity training for the experimental group and was administered to both the control and experimental groups from December 07, 2020 to December 10, 2020 as the posttest. The responses were downloaded from the online database into a Microsoft Excel spreadsheet. The participants' email addresses were used to identify the members of the control group and the experimental group.

Study Results

Research Question 1 and Hypothesis 1

RQ1 was "What is the level of cybersecurity awareness and knowledge in the public sector of the Commonwealth of Dominica?" This research question was intended to establish through descriptive statistics a quantified baseline understanding of the level of cybersecurity awareness for all participants, and to identify any differences between the two groups.

$H_0$1: There is no difference in the level of knowledge and use of cybersecurity between the control and experimental groups during the pretest.

$H_0$1: $\mu_C = \mu_E$ (where μ_C is the mean score for the control group, and μ_E is the mean score for the experimental group)

H_{a1}: There is a difference in the level of knowledge and use of cybersecurity between the control and experimental groups during the pretest.

H_{a1}: $\mu_C \neq \mu_E$

Statistical Assumptions

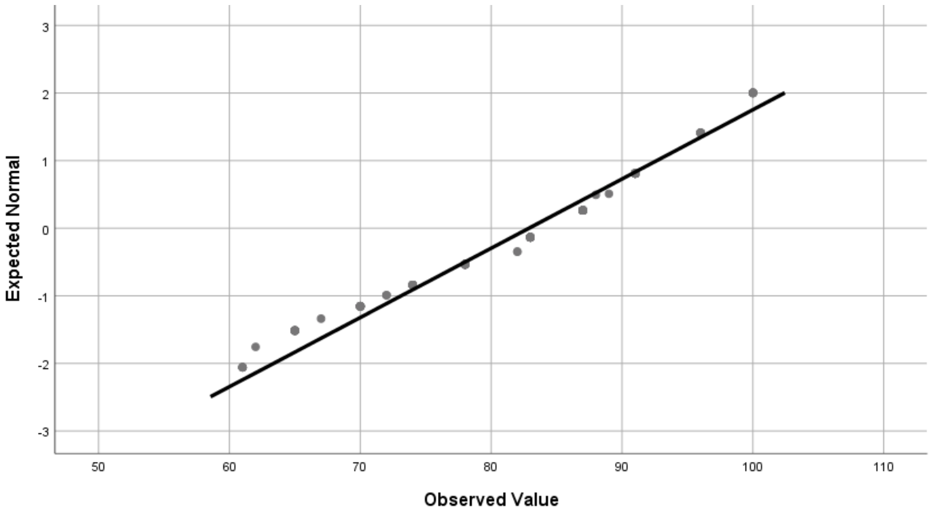
I tested the hypothesis using an independent samples *t* test. The assumptions for the *t* test are independence, numerical DV with interval or ratio measurement, normal distribution of the DV, and homogeneity of population variances of the pretest scores.

Independent and Random Samples, Continuous Numerical DV. A random sample was performed to fill the bins for both the control and the experimental groups. Consequently, there was no connection between the participants of both groups. Hence the sample data were independent and random. The scores were measured by counting the points scored, resulting in integer values that were subsequently calculated as a percentage of the 24 items on the risk assessment questionnaire. Consequently, the DV was a continuous numerical variable.

Normality. As depicted in Figure 2, the normal probability plot for the DV, the points were generally close to the line, indicating that the distribution was approximately normal. In any case, the independent samples *t* test is robust with respect to minor deviations from normality (Henze & Visagie, 2019).

Figure 2

Normal Q-Q Plot of Control and Experimental Groups Pretest Scores



Homogeneity of Variance. As seen in Table 6, the *p* value was equal to 0.45 which is greater than 0.05. Consequently, the null hypothesis, which states that the variance for the control group is equal to that of the experimental group, was not rejected. Therefore, I used a pooled variance *t* test; equal variance was assumed.

Table 6

F Test Two-Sample for Variances

	Variable 1	Variable 2
Mean	82.30681818	83.43678161
Variance	97.31857367	94.57444534
Observations	88	87
Df	87	86
F	1.029015537	
p (*F* <= f) one-tail	0.447412046	
F Critical one-tail	1.427437648	

Independent Samples t Test

As seen in the Table 7, the means of 82.31 and 83.48 of the pretest scores of the control and experimental group differed by 1.17. The pretest scores represent the percentage of correct responses on the risk assessment questionnaire. The overall mean score for all participants was 82.90.

Table 7

Group Statistics

	Groups	*N*	Mean	Std. Deviation	Std. Error Mean
Control and Experimental Groups Pretest Scores	Control	88	82.31	9.865	1.052
	Experimental	88	83.48	9.676	1.032

Table 8

Independent Samples Test

		t Test for Equality of Means				
		t	*df*	Sig. (2-tailed)	Mean Difference	Std. Error Difference
Control and Experimental Groups Pretest Scores	Equal variances assumed	-.795	174	.428	-1.170	1.473

In Table 8, the independent samples *t* test produced a *p* value of 0.43, which is greater than 0.05. The null hypothesis, given symbolically as $\mu_C = \mu_E$ (where μ_C is the mean score for the control group, and μ_E is the mean score for the experimental group), was not rejected. I concluded that there was no difference in the level of knowledge and use of cybersecurity between the control group and experimental group during the pretest.

Research Question 2 and Hypothesis 2

RQ2 was, what is the level of pretest cybersecurity awareness and knowledge according to demographic factors age, gender, location, and access to the internet in the public sector of the Commonwealth of Dominica? The hypotheses to be tested were as follows:

> $H_0$2. There is no difference in the level of cybersecurity awareness and knowledge according to demographic factors age, gender, location, and access to the internet in the public sector of the Commonwealth of Dominica.
>
> $H_0$2: $\beta_1 = \beta_2 = \ldots = \beta_k = 0$ (all coefficients = 0)
>
> H_a2. There is a difference in the level of cybersecurity awareness and knowledge according to at least one of the demographic factors of age, gender, location, and access to the internet in the public sector of the Commonwealth of Dominica.
>
> H_a2: at least one $\beta_j \neq 0$

Multiple Linear Regression

Dichotomous dummy variables were created for gender, location, and internet access as previously shown in Tables 2, 3, and 4.

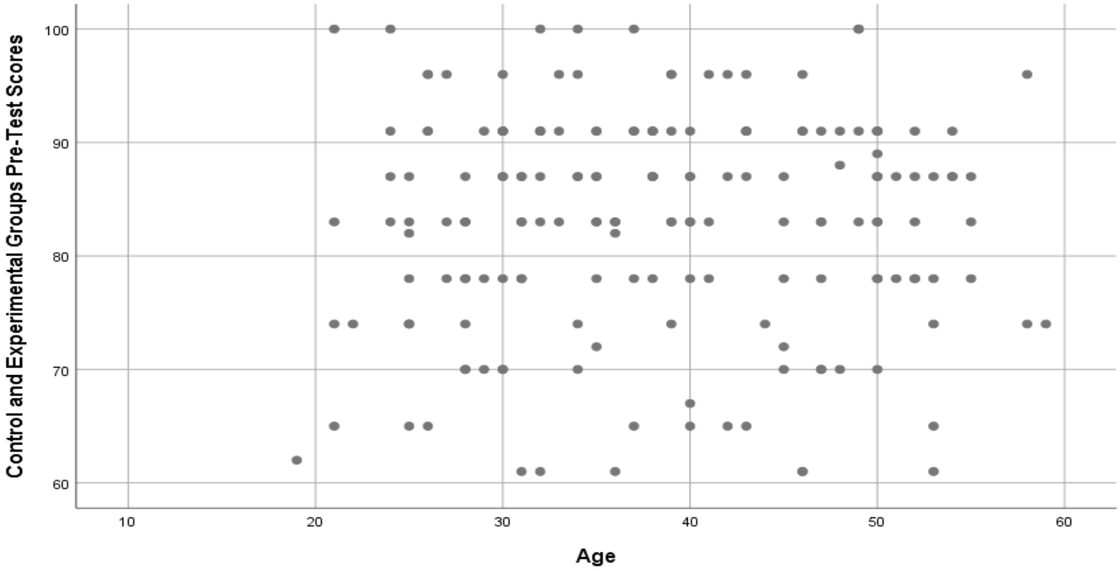
MLR Assumptions

The data were analyzed to test the assumptions for MLR. The assumptions for MLR include independence, linearity between the DV and IVs, no multicollinearity, independent and normally distributed residuals, homoscedasticity (constant variance of the residuals), and no overly influential outlier.

As seen in the scatterplot in Figure 3 depicting the pretest score, there was no non-linear pattern between the DV and age. The other three IVs were categorical in nature hence the omission of the linearity test.

Figure 3

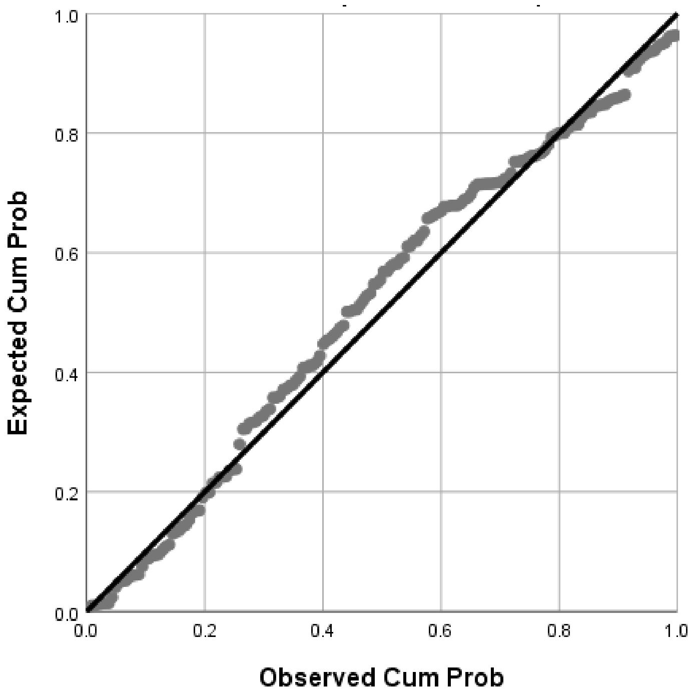
Scatterplot: Pretest Score



The Durbin-Watson statistic was 2.00. This was an indication that there was no autocorrelation detected in the sample. As seen in the normal P-P plot in Figure 4, the residuals were normally distributed.

Figure 4

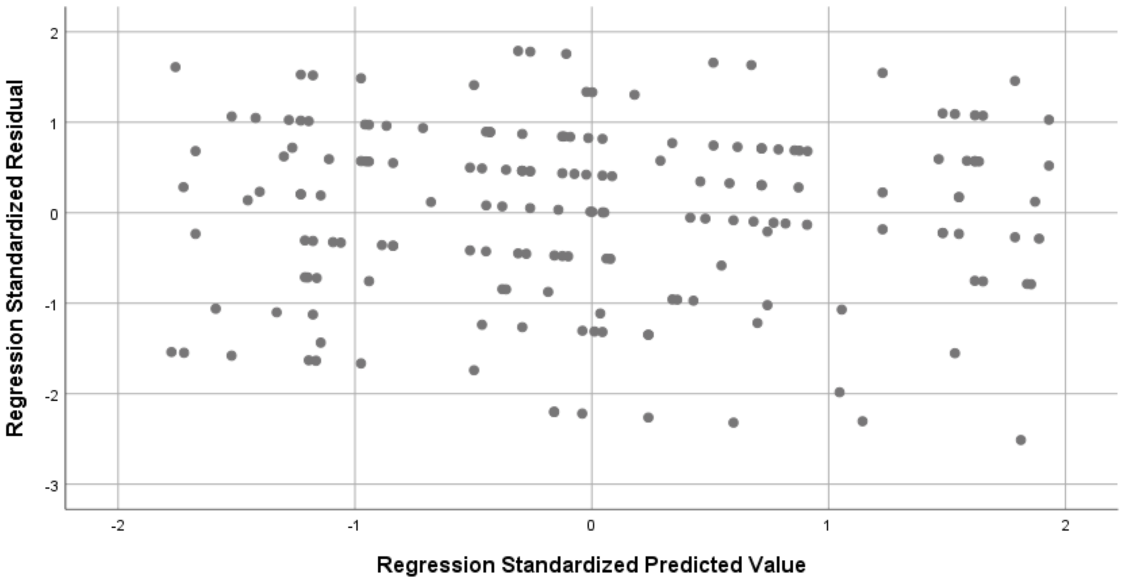
Normal P-P Plot of Regression Standardized Residual



The assumption of homoscedasticity was tested using the scatterplots of residuals for the DV as shown in Figure 5. There is no obvious pattern. The points are equally distributed above and below zero on the X axis, and to the left and right of zero on the Y axis. Consequently, the homoscedasticity assumption was not violated.

Figure 5

Scatterplot: DV: Control and Experimental Groups Pretest Scores



MLR Analysis

The original form of the model was

$$CKA = b_0 + b_1A + b_2G + b_3L + b_4I + \varepsilon.$$

However, with the creation of the dichotomous dummy variables, the form was

$$CKA = b_0 + b_1A + \beta_1 x_1 + \beta_2 x_2 + \beta_3 x_3 + \beta_4 x_4 + \beta_5 x_5 + \beta_6 x_6 + \varepsilon.$$

The null hypothesis for the test of the entire model were

H_o: $b_1 = \beta_1 = \beta_2 = \beta_3 = \beta_4 = \beta_5 = \beta_6 = 0$ (the model is not significant)

H_1: At least one coefficient is not equal to zero (the model is significant).

The criterion to reject the null hypothesis is the *p* value < 0.05.

I performed an *F* test of the regression model. As depicted in the ANOVA in Table 9, the *p* value = 0.74. I failed to reject the null hypothesis. In conclusion, there was insufficient evidence that a linear regression model constructed with the demographic variables of age, gender, location, and access to the internet is significant for predicting pretest cybersecurity knowledge.

Table 9

ANOVA

Model		Sum of				
		Squares	*df*	Mean Square	*F*	Sig.
1	Regression	421.077	7	60.154	.622	.737[b]
	Residual	16251.872	168	96.737		
	Total	16672.949	175			

Note: a. DV: Control and Experimental Groups Pretest Scores

b. Predictors: (Constant), Age(A), PreFemale(x_1), PreUrban(x_2), PreCity(x_3), PreFair(x_4), PreGood(x_5), PreExcellent(x_6)

The results of the test of the significance of each coefficient are displayed in the coefficients in Table 10. The associated null and alternative hypotheses were given by H_o: $\beta_i = 0$ (the IV is not a significant predictor of the DV) and H_1: $\beta_i \neq 0$ (the IV is a significant predictor of the DV). None of the *p* values was less than 0.05, which leads to the conclusion that none of the IVs are significant predictors of knowledge.

Table 10

Coefficients

		Unstandardized Coefficients		Standardized		
		Coefficients				
Model			Std.	Beta		
		B	Error		*t*	Sig.
1	(Constant)	82.398	6.093			
	A	.026	.078	.026	.337	
						.737
	x_1	-2.728	1.571	-.135	-1.737	.084
	x_2	.211	1.700	.011	.124	.901
	x_4	-.187	5.341	-.007	-.035	.972
	x_5	1.768	5.101	.091	.347	.729

x_6	.397	5.208	.019	.076	.939
x_3	.591	2.186	.023	.270	.787

Note: a. DV: Control and Experimental Groups Pretest Scores

Further proof that the model is not a good predictor of cyber security knowledge is given by the adjusted R^2 of -0.15 in Table 11. Since the adjusted R^2 was a negative value, it is statistically acceptable to consider it equal to zero. Hence, the adjusted R^2 confirmed that none of the changes in the DV can be attributed to a model comprised of these IVs.

Table 11

Model Summary

Model	*R*	*R* Square	Adjusted *R* Square	Std. Error of the Estimate	Durbin-Watson
1	.159[a]	.025	-.015	9.836	1.973

Notes: a. Predictors: (Constant), Age(*A*), PreFemale(x_1), PreUrban(x_2), PreCity(x_3), PreFair(x_4), PreGood(x_5), PreExcellent(x_6)

b. DV: Control and Experimental Groups Pretest Scores

The *p* value for x_1 was .084, which indicates potential for significance. Therefore, I performed an additional regression analysis (Table 12) of the DV as a function of only x_1.

Table 12

Model Summary

					Change Statistics				
Model	*R*	*R* Square	Adjusted *R* Square	Std. Error of the Estimate	*R* Square Change	*F* Change	*df*1	*df*2	Sig. *F* Change

1	.017[a]	.000	-.005	13.970	.000	.048	1	177	.826

Notes: a. Predictors: (Constant), PreFemalex1

b. DV: Control and Experimental Groups Pretest Scores

Table 13

ANOVA

Model		Sum of Squares	df	Mean Square	*F*	Sig.
1	Regression	9.430	1	9.430	.048	.826[b]
	Residual	34543.408	177	195.160		
	Total	34552.838	178			

Notes: a. DV: Control and Experimental Groups Pretest Scores

b. Predictors: (Constant), PreFemalex1

It can be seen from Table 12 that the adjusted R^2 was approximately zero. In Table 13, it can be observed that the *p* value was 0.826 > 0.05. This is an indication that the model containing only gender as a predictor is not a good fit. Since age was the only numerical variable in the model, further analysis was conducted.

Table 14

Correlations

		Age of the Experimental Group	Experimental Group Posttest Score	Experimental Group Pretest Score
Age of the Experimental Group	Pearson Correlation	1	.065	-.058
	Sig. (2-tailed)		.548	.592
	N	88	88	88

According to Table 14, there was a very weak positive and weak negative correlation between age and pretest, and age and posttest scores, respectively. Both the *p* values were greater than 0.05. As a result, I did not rejection the null hypothesis which stated that there was no correlation between age and posttest scores. This suggests that the age of the employees demonstrated no significant influence on the level of cybersecurity knowledge.

Research Question 3 and Hypothesis 3

RQ3 was, does a training intervention impact the level of knowledge and use of cybersecurity?

$H_0$3. The experimental group demonstrates a level of knowledge and use of cybersecurity equal to or lower than the control group as measured during the posttest.

$H_0$3: $\mu_E \leq \mu_C$ (where μ_C is the mean score for the control group, and μ_E is the mean score for the experimental group)

H_a3. The experimental group demonstrates a higher level of knowledge and use of cybersecurity than the control group as measured during the posttest.

H_a3: $\mu_E > \mu_C$

Statistical Assumptions

The assumptions for the *t* test are independent and random samples, numerical DV with interval or ratio measurement, normality of the DV distribution, and homogeneity of population variances of the pretest scores.

Independent and Random Samples, Continuous Numerical DV. I performed a random sample to fill the bins for both the control and the experimental groups independently. Consequently, there is no connection between the participants of both groups. Hence their sample data are independent and random. The scores were measured by counting the points scored on the risk assessment questionnaire, giving rise to integer values. Consequently, the DV was a continuous numerical variable.

Normality. According to the following Q plots for the posttest scores for the control and experimental groups in Figure 6 and Figure 7, the points are generally close to the line, indicating that both distributions are close to normal. However, the independent samples *t* test is robust with respect to small deviations from normality (Henze & Visagie, 2019).

Figure 6

Normal Q-Q Plot of Control and Experimental Groups–Posttest Scores: Control

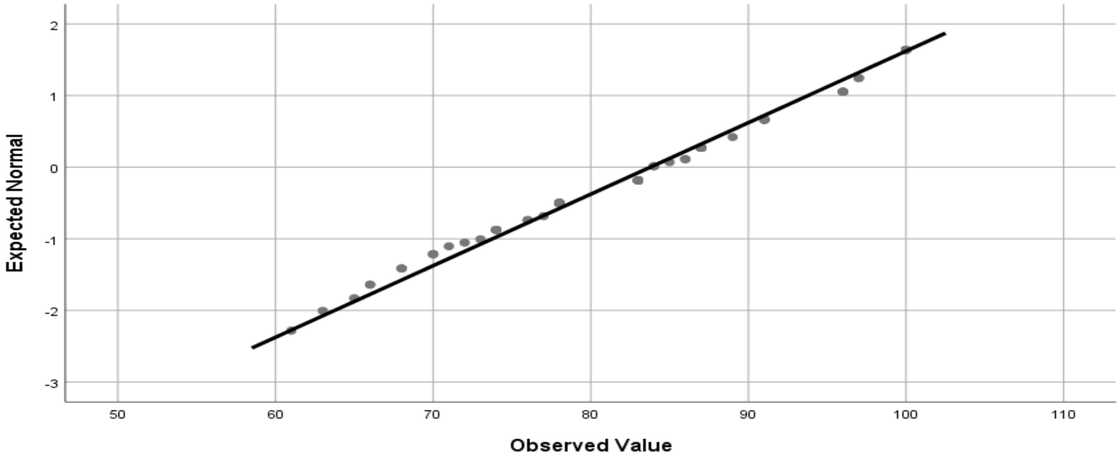
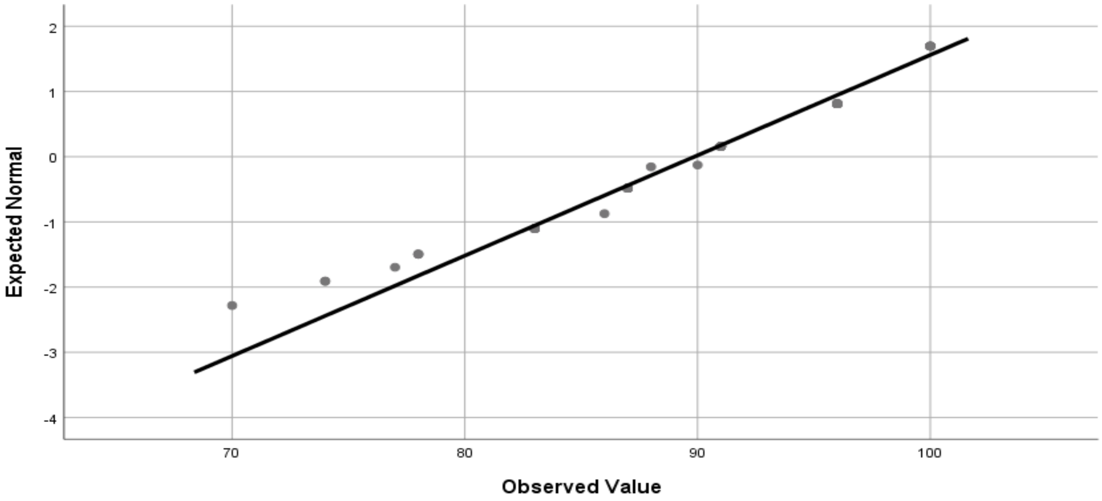


Figure 7

Normal Q-Q Plot of Control and Experimental Groups – Posttest Scores: Experimental



Homogeneity of Variance. As seen in Table 15, the *p* value was equal to 4.88×10^{-5} which is smaller than 0.05. Consequently, I rejected the null hypothesis, which states that the variances for the control group is equal to that of the experimental group. Hence the assumption of the homogeneity of variance was violated. For this reason, to test the hypothesis I used a separate variance *t* test.

Table 15

F Test Two-Sample for Variances

	Variable 1	Variable 2
Mean	83.77272727	89.85057471
Variance	100.2236155	42.68671478
Observations	88	87
Df	87	86
F	2.347887767	
p (*F* <= f) one-tail	4.87923E-05	
F Critical one-tail	1.427437648	

Independent Samples Tests

As seen in Table 16, the means for the pretest scores of the control and experimental group differed by 6.09. The experimental group scored 6.09% higher than the control group during the posttest.

Table 16

Group Statistics

	Groups	N	Mean	Std. Deviation	Std. Error Mean
Control and Experimental Groups Posttest Scores	Control	88	83.77	10.011	1.067
	Experimental	88	89.86	6.497	693

Table 17

Independent Samples Test

		t Test for Equality of Means				
		t	*df*	Sig. (2-tailed)	Mean Difference	Std. Error Difference
Control and Experimental Groups Posttest Scores	Equal variances assumed	-4.788	174	.000	-6.091	1.272
	Equal variances not assumed	-4.788	150	.000	-6.091	1.272

The null hypothesis, given symbolically as $\mu_C = \mu_E$ (where μ_C is the mean score for the control group, and μ_E is the mean score for the experimental group). If the *p* value < 0.05 the null hypothesis is rejected. In Table 17, the *t* statistic and *p* value were -4.79 and 0.00 respectively. Consequently, the null hypothesis was rejected. Hence, there was sufficient evidence that the alternative hypothesis is true: There is a difference in posttest knowledge between the experimental and control group.

Research Question 4 and Hypothesis 4

RQ4: Is there a change or increase in the level of knowledge and use of cybersecurity for the experimental group from the pretest to the posttest?

$H_0$4. There is no change or a decrease in the level of knowledge and use of cybersecurity for the experimental group from the pretest to the posttest.

$H_0$4: $\mu_D \leq 0$ (where μ_D is the mean difference of scores for the participants in the experimental group, from pretest to posttest)

H_a4. There is an increase in the level of knowledge and use of cybersecurity for the experimental group from the pretest to the posttest.

H_a4: $\mu_D > 0$

The hypothesis was tested using the paired *t* test. This test compared the scores of the experimental group from pretest to posttest.

Statistical Assumptions

The assumptions for the paired *t* test are independent and random samples, numerical DV with interval or ratio measurement, normality of the DV distribution, and homogeneity of population variances of the pretest scores.

Random samples. A random sample was performed to fill the bins for both the control and the experimental groups in an independent basis. Consequently, the samples were random and independent.

Numerical dependent variable. The scores were converted to a percentage. Consequently, the DV was a continuous numerical variable.

Normality. As shown in Figure 9, normal Q - Q plot for the difference in the pretest and posttest scores for the experimental group, the points are generally close to the line, indicating that both distributions are close to normal. This approach to normality by the difference in pre and posttest scores is further depicted in the histogram in Figure

10. However, the independent samples *t* test is robust with respect to small deviations from normality (Henze & Visagie, 2019).

Figure 8

Normal Q-Q Plot of Difference Pre and Post Experiment

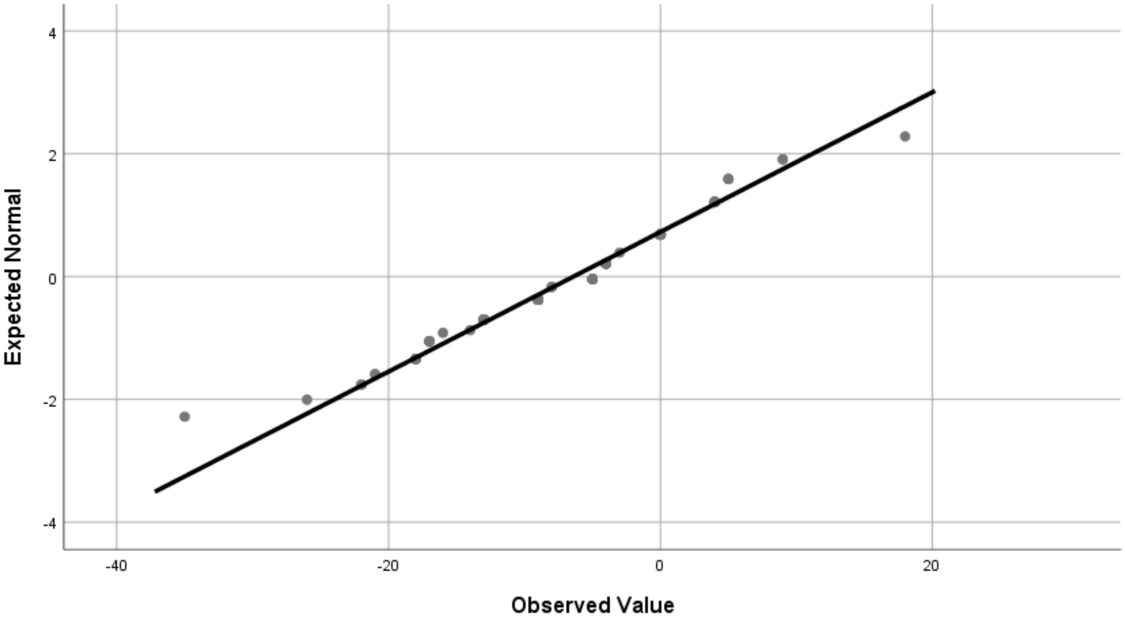


Figure 9

Histogram: Difference Pre and Post Experiment

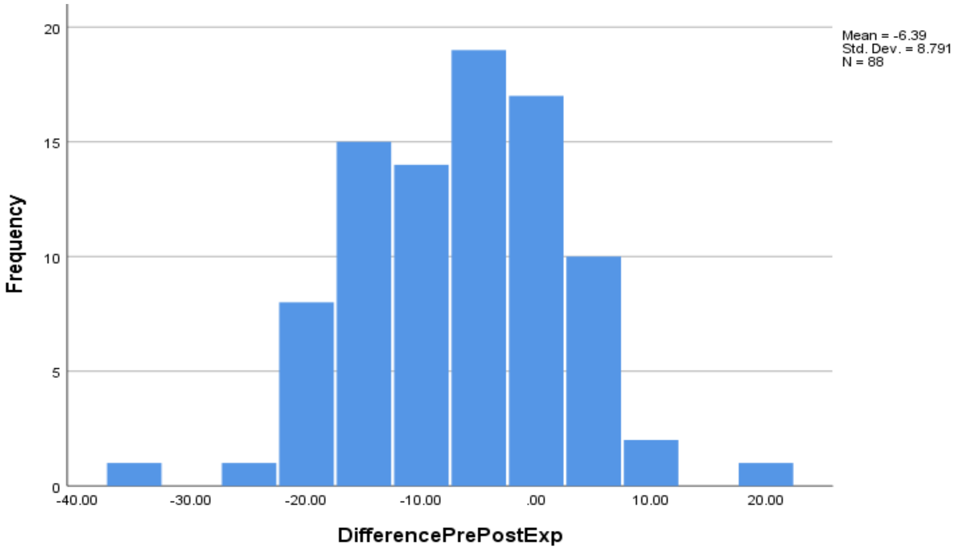


Table 18

Paired Samples Test

		Paired Differences							
					95% Confidence Interval of the Difference				
		Mean	Std. Deviation	Std. Error Mean	Lower	Upper	*t*	*df*	Sig. (2-tailed)
Pair 1	Experimental Group Pretest Score - Experimental Group Posttest Score	-6.386	8.791	.937	-8.249	-4.524	-6.815	87	.000

The null hypothesis states that the mean difference of the scores for the participants in the experimental group, from pretest to posttest is less than or equal to zero. This is symbolically written as $\mu_D \leq 0$. The decision criteria states that if the *p* value < 0.05, the null hypothesis is rejected. The *t* statistic and *p* value were -6.82 and 0.00 respectively. Consequently, the null hypothesis was rejected. Hence, there was sufficient evidence that the alternative hypothesis is true: The mean difference between the posttest and pretest scores for the experimental group was greater than zero. The test showed that the average difference was a 6.39% improvement from pretest to posttest.

Summary

The purpose of this study was to explore the role and effectiveness of employee training focused on user awareness of cyberattacks and cybersecurity, with the intent to close the gap in understanding about the level of awareness of cybersecurity within the public sector of the Commonwealth of Dominica. The instrument used in this study was a questionnaire which measured the cybersecurity awareness and knowledge of respondents within the public sector of the Commonwealth of Dominica. I used a random sampling with stratification on the two variables of age and gender. I collected data over 10 weeks to include a pretest and a posttest. I collected 176 questionnaire responses. I considered four demographic variables in the study and used SPSS and Microsoft Excel to analyze the data collected.

There was a deviation in the actual cybersecurity training when compared to the plan that was outlined in Chapter 3. This was a result of the global pandemic COVID-19 affecting countries including the Commonwealth of Dominica. However, the statistical analysis was conducted as planned and outlined in Chapter 3.

RQ1: The control and experimental groups were independently and randomly constructed and both demonstrated equal performance on the pretest. There was no significant difference in the level of knowledge and use of cybersecurity between the control group and experimental group during the pretest; the two groups had equal knowledge.

RQ2: The results showed that a linear model of the demographic factors age, gender, location, and access to the internet in the public sector were not reliable predictors of cybersecurity awareness and knowledge. Furthermore, a model with gender as the sole predictor was not a significant predictor.

RQ3: There was a significant difference in the level of knowledge and use of cybersecurity between the control group and experimental group during the posttest.

RQ4: There was sufficient evidence to conclude that the cybersecurity knowledge after the training for the experimental group was greater.

I will interpret the results in Chapter 5. Chapter 5 also includes the limitations of the study, the generalizability of the study results, limitations to trustworthiness, recommendations for further research, and implications for potential impact for positive social change.

Chapter 5: Discussion, Conclusions, and Recommendations

This chapter provides an interpretation of the findings from Chapter 4 and compares them with previous scholarly research described in Chapter 2. I address limitations of the study, offer recommendations for future research, and discuss the implications for positive social change. I conclude with recommendations for practice.

The purpose of this quantitative experimental study was to explore the role and effectiveness of employee training focused on user awareness of cyberattacks and cybersecurity, with the intent to close the gap in understanding about the level of awareness of cybersecurity within the public sector of the Commonwealth of Dominica. The pre-and post-quantitative analysis examined the degree to which the scores for the participants who received the cybersecurity training differed from those who did not receive the cybersecurity training. The target population of this experimental study consisted of employees within the public sector of the Commonwealth of Dominica. The study results provide the public sector of the Commonwealth of Dominica a baseline understanding of the level of awareness that currently exists and the extent to which training impacted the level of employee knowledge of cybersecurity threats, which could ultimately reduce the volume of cyberthreats.

The key finding was that a linear model of the demographic factors age, gender, location, and access to the internet in the public sector were not reliable predictors of cybersecurity awareness and knowledge and that a model with gender as the sole predictor was not a significant predictor. Other key findings were that the control and experimental groups were independently and randomly constructed, and both demonstrated equal performance on the pretest; there was no significant difference in the level of knowledge and use of cybersecurity between the control group and experimental group during the pretest. There was also sufficient evidence to conclude that the cybersecurity knowledge after the training for the experimental group was greater.

Interpretation of Findings

Research Question 1

RQ1 was "What is the level of cybersecurity awareness and knowledge in the public sector of the Commonwealth of Dominica?" Cybersecurity knowledge and understanding by employees within the public sector of the Commonwealth of Dominica was measured as the score on a test of awareness and knowledge of cybersecurity. The results indicated that there was no difference in the level of knowledge and use of cybersecurity between the control group and experimental group during the pretest.

More importantly, the results revealed that before the cybersecurity training, the knowledge and understanding of cybersecurity by employees in the public sector of the Commonwealth of Dominica was low with a mean score of 83%. The pre assessment tool, in preparation for the Security Awareness TrainingPack Courses administered as the pretest before the first day of class, defined cybersecurity awareness as low with a score below 85, medium with a score between 86-94, high with a score of 95 and above. Low awareness was further defined as ignoring security alerts provided by software applications or security policies. A medium cybersecurity awareness level includes improper technology use, and a high awareness includes having knowledge and awareness of cyberthreats, and the ability to take the necessary actions to prevent a cyberattack.

In my research, only 30% of employees in the pretest provided the correct answer for the item on questionnaire, “Which of the following could indicate a phishing attempt in an e-mail message, even if logos and images make the message appear to be from a trusted source?” While the public sector of the Commonwealth of Dominica often showed responsibility by installing antivirus and other protective software on computers and servers, prior studies have shown that installing protective software does not totally mitigate against cyberthreats or cyberattacks (e.g., Khalid et al., 2018). This is because employee error remains the weakest link in a possible cyberattack or breach (Hua & Bapna, 2013). My study results are supported by prior research that employees’ lack of knowledge and awareness of cybersecurity may pose a liability for information systems (Arquilla & Guzdial, 2017). The results of my study and prior research show that employees have a basic understanding of the term *cybersecurity* as well as an understanding that a cyberattack can cause loss of money through online fraud or personal identity theft. However, my results demonstrated that only a few employees, less than 50%, were able to engage in more sophisticated activities to protect themselves against a cyberattack or cyberthreats. In my research, the results revealed that 90% of employees were able to identify what constitutes a strong password in response to the questionnaire item, “Which of the following is the most secure password?” While the overall results showed that there was no difference in the level of cybersecurity awareness and knowledge in the public sector of the Commonwealth of Dominica.

Research Question 2

My study explored the effect that demographic factors such as age, gender, location, and access to the internet in the public sector had on cybersecurity awareness and knowledge of employees in the public sector of the Commonwealth of Dominica. The results showed that the demographic factors age, gender, location, and access to the internet in the public sector were not reliable predictors of cybersecurity awareness and knowledge.

I performed an additional regression analysis of gender. Research by Anwar et al. (2017) found that gender had little effect on cybersecurity behaviors. This supports the results of my study which revealed that a model with only gender was not a significant predictor of cybersecurity awareness.

A noteworthy observation is that 63.6% of the participants in my study were female as compared to 36.4% male. In prior research, Anwar et al. found that men had slightly higher self-reported cybersecurity behavior. This differs from previous research of Tsai et al. (2016) and Webb et al. (2014) in that it revealed that women were more concerned about vulnerability than men and, therefore, were more likely to have a higher knowledge and awareness of cybersecurity. However, my results did not show a difference in awareness by gender.

My study confirmed previous research (e.g., Purkait et al., 2014) reporting that gender and age did not have a significant effect on the cybersecurity knowledge and awareness of employees. This contradicts the results of previous research regarding the interactions of demographic factors such as age and gender as having a significant effect on cybersecurity knowledge and awareness. For example, Krishan (2018) found that age and gender were significant demographic variables as it related to cybersecurity awareness.

The fact that females outnumbered males in my research could have affected the demographic factor gender as not having a significant effect on knowledge and cybersecurity. However, the essential outcome here was that demographic factors are not associated with cybersecurity awareness.

I evaluated the demographic factor of age to determine if it had any significant influence on cybersecurity knowledge and awareness. My findings revealed that age had no significant effect on cybersecurity knowledge and awareness. Furthermore, and based on the results, it can be inferred that the age group between 41-60 might have little or no knowledge of cybersecurity. This was supported by Carlton and Levy (2015) who found that older persons were more skeptical in using the internet for online transactions. The fear of identity theft was a common fear of older persons when using the internet and this was manifested in their limited cybersecurity awareness and knowledge. On the other hand, Khalid et al. (2018) revealed that younger persons were more susceptibility to cyberthreats and cyberattacks because of their general lack of experience and concern for the dangers associated with the internet.

Research Question 3 and Research Question 4

RQs 3 and 4 were both focused on whether training increases cybersecurity awareness. The findings of my study showed that there was a significant difference in the level of knowledge and use of cybersecurity between the control group and experimental group during the posttest. This is one indication that the cybersecurity intervention was effective in increasing the level of knowledge and use of cybersecurity for employees in the public sector.

In addition, my findings found that the level of awareness of the experimental group after the training was medium (with a mean score of 89%) according to the ratings provided by the pre assessment tool used as part of the cybersecurity training course. This was a second indication that cybersecurity training increased awareness about cybersecurity among employees in the public sector. This is consistent with previous studies (e.g., Udroiu, 2018) that training contributes to raising the cybersecurity awareness of employees within organizations. Khalid et al. (2018) found that cybersecurity training contributes to the individual's cybersecurity awareness after using an all-encompassing survey that was designed to assess the participants' awareness before and after an intervention. Prior research (e.g., Yoo et al., 2018) found that increasing cybersecurity awareness empowers employees with the knowledge needed to detect cyberthreats as well as the ability to detect cyberattacks and, hence, being able to take actions that will mitigate against becoming a victim. My findings contradicted previous research of Boss et al. (2015) who concluded that cybersecurity training is not an effective measurement of cybersecurity knowledge and awareness but, rather, a more scientific approach was needed.

Additionally, my research results highlighted that there are gaps in the cybersecurity knowledge that can be significantly improved by exposing employees to cybersecurity training. This was refuted in prior research by Taitto et al. (2018) who maintained that cybersecurity is more about employee's behavior than it is about training or building knowledge. However, where Taitto's assertion was faulty is that behavior may very well be changed by training, my study dovetailed with the work of previous researchers (e.g., de Bruinjn & Janssen, 2017) who promoted the concept that cybersecurity awareness can be developed through workshops and collaboration so that they develop the necessary knowledge and awareness to protect themselves from the growing threats of cyberattacks.

Prior to the training intervention in my research, 74% of the employees in the experimental group responded correctly to the following item on the questionnaire, "Which of the following is the best advice about passwords?" However, after the training intervention, 94% of the employees in the experimental group responded correctly to the question. On the other hand, as it relates to the items in the questionnaire under the category *protecting and handling data*, the scores of the employees in the experimental group remained between 60% and 62%. The results are significant in that employees' level of cybersecurity knowledge and awareness as it relates to the ability to protect the information and data of the public sector remained low. In the literature review, I noted that Sans (2019) reported that one in five individuals is a victim of online fraud that resulted in losses of over $2.6 billion per year. The results of my study support the assertion that the likelihood of an increase in the success of cyberattacks due to limited cybersecurity awareness and knowledge of employees, which can cause significant interruptions and financial losses to the government of the Commonwealth of Dominica, can be attributed to employees.

Influence of SCT

Employees' behavior can be explained by applying the SCT. The SCT explains the capabilities of an individual to execute a course of action that is required to attain a desired objective (Carillo, 2010). Bandura (1989) alluded to several SCT concepts that influence employee behavior, including behavioral capability which can be described as having the understanding and knowing the skills necessary for employees to perform a behavior or task. Previous research, including Brown (2015), reported that employees who have been exposed to cybersecurity awareness training tend to be more inclined to protect the information systems by emulating what was learned or observed during the training. In other words, an employee who has cybersecurity awareness and knowledge will assess the cyberthreats and then use the most effective measure to address the potential cyberthreat.

Further analysis of my findings also confirms that the concept of behavioral capability is interconnected with the employees' knowledge to perform a behavior and that the action, cybersecurity training, has a positive effect on the cybersecurity posture of the group—in this case, the public sector of the Commonwealth of Dominica. Thus, based on the findings in my research, it appears that the managers of the public sector can design specific and repeated cybersecurity training that incorporates practical scenarios on cyberthreats and cyberattacks that employees can emulate in securing information systems and applications within the public sector.

My research adds to the body of knowledge on SCT as articulated by Moody and Siponen (2013) that the environment and social cognition influence the behavior and perspectives of employees in relation to cybersecurity. Further, my research does not refute existing literature on the central concept of Bandura’s (2001) SCT that pertains to an employee’s ability to perform a behavior through knowledge and skills (as described by Gonçalves de Lima et al., 2020) and highlighted in Chapter 2.

Limitations of the Study

Limitations to Generalizability

My research, like other research, has several limitations. As it relates to gender, only 36% of the sample was male, the findings may not be a completely accurate representation of males in the target population, the public sector of the Commonwealth of Dominica. Prior research (see Shillair et al., 2016) alluded to the fact that women tend to be more concerned about cybersecurity issues than men and, therefore, were more likely to adhere to security policies than men. While gender had no significant effect on cybersecurity knowledge in my research, it would be important to know whether a larger male sample would have had any significant effect on the research.

The length of the cybersecurity training and the demand for a level of computer skills could be viewed as limitations. The experimental period of the study lasted only 4 weeks. At the point that the participants began to understand and apply the practical activities of the cybersecurity training, the training period came to an end. While the participants had the basic computer knowledge to participate in the training, not all the participants were at the same level of computer awareness and knowledge. Some of the participants required additional time for retention of skills, more time to practice, and more time to get accustomed to the training material. This limitation may have had an impact on the participants’ scores for the posttest which although was higher than the pretest, still many of the participants scored lower than 85%.

Further, in completing the risk assessment questionnaire, there was the limitation of the participants’ ability to comprehend the items in the risk assessment questionnaire which could also be attributed to the limitation of the duration of the training. I conclude that if the participants had more time to understand the material and do the practice sessions, they would have better understood and responded to the items in the risk assessment questionnaire.

Additionally, the risk assessment questionnaire lacked flexibility in that the only information gathered was the responses to the questions in the risk assessment questionnaire without an opportunity for follow up questions. The risk assessment questionnaire did not measure other factors that could have had an impact on the cybersecurity awareness and knowledge such as the commitment of the public sector governance in alleviating cybersecurity risks, peer pressure, and social influence on the participants who completed the risk assessment questionnaire. These limitations may have impacted the responses given by the participants and possibly affected the results of the study. In the recommendations section, I will provide some ideas for research to overcome these limitations.

Limitations to Trustworthiness

The study was completed as described in the approved proposal, with the exception of completing the training online due to the Covid-19. There was no incentive for the participants to complete the instrument and, therefore, there is no indication in the results that would suggest that the participants did not honestly complete the instrument. Given my background and knowledge of information technology and cybersecurity in the public sector, my general assessment of the results of the risk assessment questionnaire is that the participants completed the risk assessment questionnaire honestly. Therefore, the results of the risk assessment questionnaire can reasonably be trusted.

Recommendations

The purpose of these recommendations is to assist in furthering the research on user awareness and knowledge of cybersecurity in the public sector of the Commonwealth of Dominica. The recommendations are based on the methodology, limitations of the study, and the literature review.

Future research might include the private sector of the Commonwealth of Dominica, randomly assigning the private sector and the public sector into a control group and an experimental group. Results more representative of the entire population might be achieved by including private sector participants.

My research provided an opportunity to explore the impact of training on user awareness and knowledge of cybersecurity. Most previous research indicated that user awareness and knowledge of cybersecurity requires a closer look into the methods as well as the frequency in which cybersecurity training is delivered (see, for example, Zak & Ware, 2020). In this study, the cybersecurity training was done fully online. Future research might explore the benefits of more traditional cybersecurity awareness and knowledge training. A traditional classroom setting would provide a greater benefit to participants by allowing for in-class practical demonstrations (Bauer & Bernroider, 2017). However, there are advantages to having more people participate in online training and avoiding the limitation of space associated with in-person training. Further, a longer training period would provide the opportunity for participants to get better opportunity to fully understand the training material. By identifying which of the training course contents resonated with the participants, it will be possible for the public sector to develop targeted cybersecurity awareness training around that particular training course content.

My research focused on four demographic factors that could have an impacted the knowledge and awareness of cybersecurity for employees in the public sector. Future research might assess other factors such as education to determine their effect on cybersecurity awareness and knowledge. The cybersecurity awareness training in my research utilized an online computer-based training program. The targeted population was between the ages of 18 to 60 years old. The training was not tailored to any specific age group and thus participants who may not have been exposed to cybersecurity knowledge or training from previous educational setting would have had a higher learning curve than the other participants. In future research, training might target specific users based on age grouping.

Future research could target senior management, ministers of government, and national employment appointees as users. Future research could also examine factors that go beyond the user including political support and government policies on the use of information and communication technologies. In addition to this, further research can provide meaningful information on factors that can weaken any cybersecurity system implemented by the public sector of the Commonwealth of Dominica. Some of these factors may be lack of proper working conditions, job security, and employee satisfaction. This research can guide the managers in creating the environment for effective management of cybersecurity policies and systems.

Further, governments have invested most of their resources into installing physical security against cybersecurity and cyberattacks with little or no investment in training employees (Rahim et al., 2015). According to Wall and Buche (2017), a major component of information security is creating an understanding and knowledge pool on cybersecurity and other security risks, by providing continuous education to employees on the risk associated with cyberthreats and cyberattacks. Gascó (2017) proposed that if employees had a greater degree of knowledge and awareness of cyberthreats and cyberattacks, those employees will engage in behaviors that can enhance the cybersecurity of information systems.

Lastly, I recommend that future research be conducted to better understand other factors that could have had an impact on the cybersecurity awareness and knowledge. These factors might include commitment of the public sector governance in alleviating cybersecurity risks, peer pressure, and social influence on employees within the public sector of the Commonwealth of Dominica.

Implications

Potential Impact for Positive Social Change

The potential positive impact of my research on society is significant in that it heightens the awareness of cyberthreats. And, it reinforces the notion that investing in training has the potential for significant benefits to organizations and people.

With increased knowledge and understanding of cybersecurity through training, employees of the public sector of the Commonwealth of Dominica would be able to identify a cyberthreat and to take actions that can mitigate against cyberthreats and cyberattacks. Employees with a greater cybersecurity awareness would be more careful with how they use the internet and the information systems of the public sector.

As a result of my research, managers of the public sector who are contemplating investing in upgraded information systems, might also consider investments in cybersecurity training. Such training would provide managers the confidence that the employees are more capable of preventing cyberattacks and cyberthreats on the upgraded systems as a result of the training that exposed them to the threats posed by opening unsolicited emails or using open WiFi to access the network of the public sector. This is beneficial because the public sector recently signed a contract with the World Bank valued at $28 million to digitize key services within the public sector. It is therefore necessary to have a workforce that is able to understand the risk posed by having online services. My research is one step toward enhancing that understanding.

Information and communication technology has the potential to transform the delivery of service and products within the public sector of the Commonwealth of

Dominica which in turn can positively affect social change by reducing transactional time and cost for businesses and the public. This study assisted in unraveling the risks that employees did not often associate with cybersecurity that had the consequences of curtailing the adoption of technology as part of the delivery of services and products. Further, the findings have provided a platform for other stakeholders in the Commonwealth of Dominica to discuss how the risks associated with cybersecurity can be mitigated in order to enhance their own success rate of delivery of service by adopting technology to enhance positive social change, and to build confidence in the safety, and security of business data and the personal information of users of the internet.

Implications for Professional Practices

The focus of my study was on user awareness and knowledge of cybersecurity. Chen and Dongre (2014) pointed out that the user is a contributor towards the risk of cyberattacks. The public sector of the Commonwealth of Dominica is the largest employer in the Commonwealth of Dominica; therefore, ensuring that users are compliant with cybersecurity requirement to protect information technology systems can be considered as one of the most important strategic objectives that can be implemented within the public sector of the Commonwealth of Dominica.

Previous research found that although there were many research studies that identified cybersecurity awareness and knowledge as a problem within the region and more specifically, the Commonwealth of Dominica, there was little or no research done on implementing a cybersecurity training intervention that solved this problem (Organization of American States [OAS], 2018). One of the most practical implications of my study is that the training materials can be further developed into a standard training course that is administered to all employees of the public sector of the Commonwealth of Dominica every 6 months. The training materials used in the study were practical scenarios of every day cyberthreats and catered to non-information technology practitioners. The training materials must be such that it can be easily modified as new cyberthreats arise.

Another practical implication is that the training should be done in smaller groups to provide an opportunity for employees who may require more time to fully understand the training materials. The low responses or scores to some of the questions on the questionnaire can be attributed partly to the participants not being aware of the types of cyberthreats or how to recognize cyberthreats. Managers of the public sector can introduce on its internal portal weekly information on cybersecurity tips in the form of videos. For example, employees with limited cybersecurity awareness often use devices that are not protected to access public sector information. The use of the devices that are not protected added with limited cybersecurity awareness can be a gateway for cyber criminals and invasion of cyberthreats on the information systems of the public sector. These adjustments to training might increase the awareness and knowledge of cybersecurity for employees. Within the public sector, existing cybersecurity practices mainly focus on physical technology to detect and prevent cyberattacks as well as the risks that are associated with cyberattacks. However, it is necessary to develop additional strategies with the purpose of supporting and strengthening the strategies that already exist to include cybersecurity awareness and training programs. Further, the strategies must have the political and managerial support for incorporation into all the entities of the public sector. Most importantly, my research indicated that in order to prevent damage from cyberattacks and cyberthreats, the managers of the public sector of the Commonwealth of Dominica must consider employees as a key contributor in ensuring the security of its information systems.

A lack of a strategy-led course of action to prevent cyberattacks can negatively affect the economy, and general safety of a country. Since governments are responsible for the security of its citizen, and country, it is an acceptable conclusion that cybersecurity is the mandate of the government of the Commonwealth of Dominica. Furthermore, given that the public sector of the Commonwealth of Dominica is becoming heavily dependent on information technology, cybersecurity should be seen as a national priority. To support this, the government ought to perform strategic planning and their strategic plan ought to identify cybersecurity as a threat/vulnerability and training should be a goal in the plan as part of a holistic approach in addressing cybersecurity. In addition, the cybersecurity strategy should define a risk management methodology for assessing, and quantifying cyber risks against the potential impact and the likelihood of occurrence. The risk management approach should also include policies and procedures for handling of the various types of risks.

Implications for Theory

My study adds to the theory underpinning the body of knowledge within the cybersecurity domain by providing a better understanding of human motivation to acquire new knowledge and skills. More specifically, it will add to the existing knowledge on factors that can impact employees to acquire cybersecurity knowledge so that they will have an awareness of how to mitigate against cyberattacks and cyberthreats such as email phishing.

Conclusions

Cyberattacks have caused millions of dollars in losses to governments around the world and have exploited human vulnerabilities through identity theft and online applications (SANS, 2019). Humans have been identified as one of the most vulnerable groups who have been susceptible to cyberattacks as a result of limited cybersecurity knowledge and awareness (Chen & Dongre, 2014). Therefore, my research addressed the social problem that the lack of awareness of cybersecurity by employees within the public service and government agencies in the Commonwealth of Dominica created conditions in which cyberattacks were doing harm to the information systems. Cybersecurity knowledge and awareness is crucial for employees to combat any cyberthreats faced with. By conducting this research, I was able to establish how the level of user awareness and knowledge of cybersecurity can be impacted by targeted training.

Cybersecurity is a new territory for the public sector of the Commonwealth of Dominica where a strategic plan has not yet been developed to address cyberthreats and cyberattacks. However, advances in technology coupled with a global pandemic continue to drive the implementation for online services and the need to work from home. The increasing dependency on information systems and information technologies is seen in the increase of cyberattacks (Zak & Ware, 2020).

My research contributes to the body of literature on and knowledge of user awareness and cybersecurity including understanding of cybersecurity risks and mitigating against cyberthreats. This increased level of understanding can be attained by exposing employees to a rigorous tailored, and repetitive cybersecurity training. The results of the study provided an indication of the level of user awareness and knowledge of cybersecurity. Further, the results of this study contributed to bridging the gap between the practice and the theory. With this information, government agencies are empowered with the knowledge that can address the factors affecting cybersecurity, incorporate cybersecurity in strategic planning, and implement training with the objective of achieving a resilient cybersecurity environment.

References

Abawajy, J. (2014). User preference of cyber security awareness delivery methods. *Behaviour & Information Technology*, *33*, 236-247. https://doi.org/10.1080/0144929X.2012.708787

Abraham, S. (2011). *Information security behavior: factors and research directions.* Proceedings of the American Conference on Information Systems, Detroit (p. 462) Adams, M., & Makramalla, M. (2015). Cybersecurity skills training: An attacker-centric gamified approach. *Technology Innovation Management Review*, *5*(1), 5-14. https://doi.org/10.22215/timreview/861

Adebayo, A. O. (2012). A foundation for breach data analysis. *Journal of Information Engineering and Applications*, *2*, 17-21.

Aguinaldo, J. (2018). Internet of threats. *MEED Business Review*,74–76.

Ahmad, A., Maynard, S. B., & Park, S. (2014). Information security strategies: Towards an organizational multi-strategy perspective. *Journal of Intelligent Manufacturing*, *25*, 357-370. https://doi.org/10.1007/s10845-012-0683-0

Ahmad, A., Maynard, S. B., & Shanks, G. (2015). A case analysis of information systems and security incident responses. *International Journal of Information Management*, *35*, 717-723. https://doi.org/10.1016/j.ijinfomgt.2015.08.001

Ahmad, Z., Ong, T. S., Liew, T. H., & Norhashim, M. (2019). Security monitoring and information security assurance behaviour among employees: An empirical analysis. *Information and Computer Security*. https://doi.org/10.1108/ICS-10-2017-0073

Alavi, M., & Leidner, D. E. (2001). Knowledge management and knowledge management systems: Conceptual foundations and research issues. *MIS Quarterly*, *25*(1), 107-36. https://doi.org/10.2307/3250961

Alcaraz, C., & Zeadally, S. (2015). Critical infrastructure protection: Requirements and challenges for the 21st century. *International Journal of Critical Infrastructure Protection*, *8*, 53-66. https://doi.org/10.1016/j.ijcip.2014.12.002

Aldawood, H., & Skinner, G. (2019). Reviewing cybersecurity social engineering training and awareness programs—Pitfalls and ongoing issues. *Future Internet*, *11*(3), 73. https://doi.org/10.3390/fi11030073

Alqahtani, F. H. (2017). Developing an information security policy: A case study approach. *Procedia Computer Science*, *124*, 691-697. https://doi.org/10.1016/j.procs.2017.12.206

Andrews, L. J. and Gotz, N. (2013). United Nations Institute for Disarmament Research (UNIDIR) Report, The cyber index, international security trends and realities, center for strategic and international studies. https://www.unidir.org

Antoniou, G. S. (2018). A framework for the governance of information security: Can it be used in an organization. *SoutheastCon*, 1-30. https://doi.org/10.1109/secon.2018.8479032

Anwar, M., He, W., Ash, I., Yuan, X., Li, L., & Xu, L. (2017). Gender difference and employees' cybersecurity behaviors. *Computers in Human Behavior*, *69*, 437–443. https://doi.org/10.1016/j.chb.2016.12.040

Arora, B. (2019). Teaching cybersecurity to non-tech students. *Politics*, *39*(2), 252–265. https://doi.org/10.1177/0263395718760960

Arquilla, J., & Guzdial, M. (2017). Crafting a national cyberdefense, and preparing to support computational literacy. *Communications of the ACM*, *60*(4), 10-11. https://doi.org/10.1145/3048379

Asllani, A., White, C. S., and Ettkin, L. (2013). Viewing cybersecurity as a public good: The role of governments, businesses, and individuals. *Journal of Legal, Ethical and Regulatory Issues*, *16*(1),17-14.

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

Babbie, E. (2013). *The practice of social research.* (13th ed.). Cengage Learning.

Bandura, A. (1977). *Social learning theory.* Prentice-Hall.

Bandura, A. (1986). *Social foundations of thought and action: A social cognitive theory*. Prentice Hall.

Bandura, A. (1988). Organizational application of social cognitive theory. *Australian Journal of Management*, *13*(2),275-302. https://doi.org/10.1177/031289628801300210

Bandura, A. (1989). Human agency in social cognitive theory. *American Psychologist*, *44*(9),1175-1184. https://doi.org/10.1037/0003-066x.44.9.1175

Bandura, A. (1998). Health promotion from the perspective of social cognitive theory. *Psychology and Health, 13*(4),623-649. https://doi.org/10.1080/08870449808407422

Bandura, A. (2000). Exercise of human agency through collective efficacy. *Current Directions in Psychological Science, 9*(3),75-78. https://doi.org/10.1111/1467-8721.00064

Bandura, A. (2001). Social cognitive theory: An agentic perspective. *In Annual review of psychology*, (52), 1-26. https://doi.org/10.1146/annurev.psych.52.1.1

Bandura, A. (2004). Health promotion by social cognitive means. *Health Education & Behaviour*, *31*(2), 143-164. https://doi.org/10.1177/1090198104263660

Bandura, A. (2009). Social cognitive theory of mass communication. *Media Psychology, 3*(3), 264-299. https://doi.org/10.1207/s1532785xmep0303_03

Bauer, S., & Bernroider, E. W. N. (2017). From information security awareness to reasoned compliant action. *ACM SIGMIS Database: The Database for Advances in Information Systems*, *48*(3), 44–68. https://doi.org/10.1145/3130515.3130519

Bland, J. A., Petty, M. D., Whitaker, T. S., Maxwell, K. P., & Cantrell, W. A. (2020). Machine learning cyberattack and defense strategies. *Computers & Security*, 92. https://doi.org/10.1016/j.cose.2020.101738

Boss, S. R., Galletta, D. F., Benjamin Lowry, P., Moody, G. D., & Polak, P. (2015). What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. *MIS Quarterly, 39*(4), 837-864. https://doi.org/10.25300/misq/2015/39.4.5

Brown, T. (2015). A primer on data security. *CPA Journal, 85*(5), 58-62.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly, 34*(3), 523-548. https://doi.org/10.2307/25750690

Bystrova, B. (2017). Comparative analysis of curricula for bachelor's degree in cybersecurity in the Usa and Ukraine. *Comparative Professional Pedagogy*, *7*(4), 114–119. https://doi.org/10.1515/rpp-2017-0058

Cano-Aguilar, A. (2020). Quantitative research in a scholar practice of community intervention in northern Mexico. *Prospectiva*, *29*, 107–130.

Carcary, M., Renaud, K., McLaughlin, S., & O'Brien, C. (2016). A framework for information security governance and management. *IT Professional*, *18*(2), 22–30. https://doi.org/10.1109/mitp.2016.27

Carillo, K. D. (2010). Social cognitive theory in IS research – literature review, criticism, and research agenda. *Information Systems*, *Technology and Management. Communications in Computer and Information Science*, 20–31. https://doi.org/10.1007/978-3-642-12035-0_4

Carlton, M., & Levy, Y. (2015). *Expert assessment of the top platform independent cybersecurity skills for non-IT professionals*. Proceedings of the 2015 IEEE SoutheastCon, Ft. Lauderdale, Florida (pp. 1-6).

Case, D.O., & Given, L.M. (2016). *Looking for Information: A survey of research on information seeking, needs and behaviour.* (4th ed.). Emerald Group Publishing Ltd.

Cefaratti, M. A., Lin, H., & Wallace, L. (2011). The information security control environment. *Internal Auditor*, *68*(2), 55-59.

Central Intelligence Agency. (2015). *The world fact book: Internet users*. Washington, DC. https://www.cia.gov/index.html

Chen, H., & Dongre, R. (2014). Q&A. What motivates cyber-attackers? *Technology Innovation Management Review, 4*(10), 40-42. https://doi.org/10.22215/timreview/838

Chul H, L., Xianjun, G., & Raghunathan, S. (2016). Mandatory standards and organizational information security. *Information Systems Research*, *27*(1), 70-86. https://doi.org/10.1287/isre.2015.0607

Claydon, L. S. (2015). Rigour in quantitative research. *Nursing Standard*, *29*(47), 43. https://doi.org/10.7748/ns.29.47.43.e8820

Clinton, L. (2015). Best practices for operating government-industry partnerships in cyber security. *Journal of Strategic Security*, *8*(4), 53-64. https://doi.org/10.5038/1944-0472.8.4.1456

Cohen, J. (1988). *Statistical power analysis for the behavioral sciences.* Lawrence Erlbaum.

Conteh, N. Y., & Schmick, P. J. (2016). Cybersecurity: Risks, vulnerabilities and countermeasures to prevent social engineering attacks. *International Journal of Advanced Computer Research*, *6*(23), 31–38. https://doi.org/10.19101/ijacr.2016.623006

Cram, W. A., Proudfoot, J. G., & D’Arcy, J. (2017). Organizational information security policies: a review and research framework. *European Journal of Information Systems*, *26*(6), 605-641. https://doi.org/10.1057/s41303-017-0059-9

Creasey, J. (2013). *Cybersecurity incident response guide*. https://www.crestapproved.org/wpcontent/uploads/2014/11/CSIRProcurementGuide.pdf

Creswell, J. W. (2012). *Educational research: Planning, conducting, and evaluating quantitative and qualitative research.* (4th ed.). Merrill

Creswell, J. W. (2013). *Research design: Qualitative, quantitative, and mixed methods approaches*. Sage Publications, Incorporated.

.Dadkhah, M., Lagzian, M., & Borchardt, G. (2018). Academic information security researchers: hackers or specialists? *Science and Engineering Ethics*, 24(2), 785–790. https://doi.org/10.1007/s11948-017-9907-1

Dang-Pham, D., Pittayachawan, S., & Bruno, V. (2017). Investigation into the formation of information security influence: Network analysis of an emerging organization. *Computers & Security, 70*, 111-123. https://doi.org/10.1016/j.cose.2017.05.010

De Bruijn, H. & Janssen, M. (2017). Building cybersecurity awareness: The need for evidence-based framing strategies. *Government Information Quarterly, 34* (1), 1-7. https://doi.org/10.1016/j.giq.2017.02.007

Dekker, S. (2017). *The field guide to human error investigations.* Ashgate Publishing Company.

Digrazia, K. (2018). Cyber insurance, data security, and blockchain in the wake of the Equifax breach. *Journal of Business & Technology Law*, *13*(2), 255–277.

Dykstra, J., & Spafford, E. H. (2018). The case for disappearing cybersecurity. *Communications of the ACM*, *61*(7), 40–42. https://doi.org/10.1145/3213764

Edwards, I. (2013). *Country sector profile report – Information and communication technology unit*. www.finance.gov.dm

ESET Internet Security. (2018). *Free ESET Cybersecurity awareness training in the workplace*. https://www.eset.com/us/cybertraining

Faul, F., Erdfelder, E., Lang, A.-G., & Buchner, A. (2007). GPower 3: A flexible statistical power analysis program for the social, behavioral, and biomedical sciences. *Behavior Research Methods*, *39*(2), 175–191. https://doi.org/10.3758/bf03193146

Ferrillo, P., & Singer, R. (2015). Is employee awareness and training the holy grail of cybersecurity? *Corporate Governance Advisor*, *23*(3), 10-13.

Fietkiewicz, K. J., Mainka, A., & Stock, W. G. (2017). eGovernment in cities of the knowledge society. An empirical investigation of smart cities' governmental websites. *Government Information Quarterly*, *34*(1), 75–83. https://doi.org/10.1016/j.giq.2016.08.003

Field, A. (2013). *Discovering statistics using IBM SPSS statistics* (4th ed.). Sage Publications.

Forrester (2011). As enterprises look beyond auditing and monitoring: Look beyond native database auditing to improve security, audit visibility, and real-time protection. http://public.dhe.ibm.com/common/ssi/ecm/en/niw03042usen/NIW03042USEN.PDF

Flores, W. R., Antonsen, E., & Ekstedt, M. (2014). Information security knowledge sharing in organizations: Investigating the effect of behavioral information security governance and national culture. *Computers & Security*, *43*, 90-110. https://doi.org/10.1016/j.cose.2014.03.004

Frankfort-Nachmias, C., & Leon-Guerrero, A. (2018). *Social statistics for a diverse society*. (8th ed.). Sage Publications.

Gabriel, B. A., & Mohamed, A. (2011). Impact of globalization. *European Business Review*, *23*(1), 120-132. https://doi.org/10.1108/09555341111098026

Gascó, M. (2017). Living labs: Implementing open innovation in the public sector. *Government Information Quarterly*, *34*(1), 90–98. https://doi.org/10.1016/j.giq.2016.09.003

Glasser, D. & Taneja, A. (2017). A routine activity theory based framework for combating cybercrime. In *Identity theft: Breakthroughs in research and practice*, (pp. 69-78).

Goldberg, A. E., & Allen, K. R. (2015). Communicating qualitative research: Some practical guideposts for scholars. *Journal of Marriage and Family*, *77*(1), 3-22. https://doi.org/10.1111/jomf.12153

Gonzalez-Granadillo, G., Dubus, S., Motzek, A., Garcia-Alfaro, J., Alvarez, E., Merialdo, M., Debar, H. (2018). Dynamic risk management response system to handle cyber threats. *Future Generation Computer Systems*, *83*, 535-552. https://doi.org/10.1016/j.future.2017.05.043

Gonçalves de Lima, L., Jorge Nassif, V. M., & Maria Garçon, M. (2020). The power of psychological capital: The strength of beliefs in entrepreneurial behavior. *RAC - Revista de Administração Contemporânea*, *24*(4), 317–334.

Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Zhou, L. (2015). Increasing cybersecurity investments in private sector firms. *Journal of Cybersecurity*, *1*, 3-17. https://doi.org/10.1093/cybsec/tyv011

Government Information Service. (2020). Ministry of Health responses to COVID-19. www.news.gov.dm

Grimes, R. A. (2017). *Hacking the hacker.* Wiley.

Haeussinger, F. J., & Kranz, J. J. (2013). *Information security awareness: Its antecedents and mediating effects on security compliant behavior.* Paper presented at the International Conference on Information Systems, Milan, Italy.

Hadlington, L. (2017). Human factors in cybersecurity; Examining the link between internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon*, *3*(7), 1-18. https://doi.org/10.1016/j.heliyon.2017.e00346

Hajli, N., & Lin, X. (2016). Exploring the security of information sharing on social networking sites: The role of perceived control of information. *Journal of Business Ethics*, *133*(1), 111. https://doi.org/10.1007/s10551-014-2346-x

Halabi, T., & Bellaiche, M. (2018). A broker-based framework for standardization and management of Cloud Security-SLAs. *Computers & Security*, *75*, 59–71. https://doi.org/10.1016/j.cose.2018.01.019

Harnett, T. (2016). Protecting your most valuable assets crafting a cybersecurity strategy to guard against internal and external threats. *Chief Learning Officer*, *15*(8), 26.

Henninger, M. (2017). Government information: Literacies, behaviours and practices. *Government Information Quarterly*, *34*(1), 8–15. https://doi.org/10.1016/j.giq.2016.12.003

Henze, N., & Visagie, J. (2019). Testing for normality in any dimension based on a partial differential equation involving the moment generating function. 1–30. https://doi.org/10.1007/s10463-019-00720-8

Herjavec Group (2020). *The 2020 official annual cybercrime report.* https://www.herjavecgroup.com/the-2019-official-annual-cybercrime-report/

Hiller, J. S., & Russell, R. S. (2013). The challenge and imperative of private sector cybersecurity: An international comparison. *Computer Law & Security Review*, *29*(3), 236-245. https://doi.org/10.1016/j.clsr.2013.03.003

Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing employee compliance with information security policies: The critical role of top management and organizational culture. *Decision Sciences*, *43*, 615-660.

Hua, J., & Bapna, S. (2013). The economic impact of cyber terrorism. *In Journal of Strategic Information Systems*, *22*, 175-186. https://doi.org/10.1016/j.jsis.2012.10.004

Hwang, I., Kim, D., Kim, T., & Kim, S. (2017). Why not comply with information security? An empirical approach for the causes of non-compliance. *Online Information Review*, *41*(1), 2-18. https://doi.org/10.1108/oir-11-2015-0358

International Telecommunication Union. (2019). *Global cybersecurity index report.* https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

Ifinedo, P. (2014). Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. *Information & Management*, *51*, 69-79. https://doi.org/10.1016/j.im.2013.10.001

Istikoma, Bt Fakhri, N. F., Qurat-ul-Ain, & Ibrahim, J. (2015). Information security aligned to enterprise management. *Middle East Journal of Business*, *10*(1), 62-66. https://doi.org/10.5742/mejb.2015.92601

Jenab, K., & Moslehpour, S. (2016). Cybersecurity management: A review. *Business Management Dynamics*, *5*(11), 16

Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. *MIS Quarterly*, *34*(3), 549-A4. https://doi.org/10.2307/25750691

Jones, J., & Shashidhar, N. (2017). Ransomware analysis and defense: WannaCry and the Win32 environment. *International Journal of Information Security Science*, *6*(4), 57–69

Khalid, F., Daud, M.Y., Rahman, M. J. A., & Nasir, M.K.M. (2018). An investigation of university students' awareness on cybersecurity. *An International Journal of Engineering & Technology*, *7*(4), 11-14. https://doi.org/10.15345/iojes.2019.02.004

Ki-Aries, D., & Faily, S. (2017). Persona-centred information security awareness. *Computers & Security*, *70*, 663-674. https://doi.org/10.1016/j.cose.2017.08.001

Kim, L. (2017). Cybersecurity awareness: Protecting data and patients. *Nursing Management*, *48*(4), 16–19. https://doi.org/10.1097/01.numa.0000514066.30572.f3

Kim, S. H., Yang, K. H., & Park, S. (2014). An integrative behavioral model of information security policy compliance. *The Scientific World Journal*, *2014*,1-12. https://doi.org/10.1155/2014/463870

Kirkwood, A., & Price, L. (2013). Examining some assumptions and limitations of research on the effects of emerging technologies for teaching and learning in higher education. *British Journal of Educational Technology*, *44*, 536-543. https://doi.org/10.1111/bjet.12049

Knapp, K. J., & Ferrante, C. J. (2012). Policy awareness, enforcement and maintenance: Critical to information security effectiveness in organizations. *Journal of Management Policy and Practice*, *13*(5), 66–80

Krishan, R. (2018). Corporate solutions to minimize expenses from cybersecurity attacks in the united states. *Journal of Internet Law*, *21*(11), 16–19

Kshetri, N. (2013). Privacy and security issues in cloud security: The role of institutions and institutional evolution. *Telecommunications Policy*, *37*(4-5), 372-386. https://doi.org/10.1016/j.telpol.2012.04.011

Kumar, R., & Kaur, G. (2014). WASM -- A metric for securing a web application. *Journal of Research & Practice in Information Technology*, *46*(1), 19–29

Lai, F. Li, D., & Hsieh, C-T. (2012). Fighting identity theft: The coping perspective. *Decision Support Systems*, *52*(2), 353-363. https://doi.org/10.1016/j.dss.2011.09.002

Lee, Y., Lee, J., & Hwang, Y. (2015). Relating motivation to information and communication technology acceptance: Self-determination theory perspective. *Computers in Human Behavior*, *51*(Part A), 418-428. https://doi.org/10.1016/j.chb.2015.05.021

Lee, C., Lee, C. C., & Kim, S. (2016). Understanding information security stress: Focusing on the type of information security compliance activity. *Computers & Security*, *59*, 60-70. https://doi.org/10.1016/j.cose.2016.02.004

Leedy, P.D. & Ormrod, J. E. (2010). *Practical research: Planning and design* (9th Ed.) NYC: Merril

Natarajan, T., & Edwards, W. (2016). Institutions and values: A methodological inquiry. *Journal of Economic Issues (M.E. Sharpe Inc.)*, *50*(2), 575-583. https://doi.org/10.1080/00213624.2016.1179067

Newman, I., & Hitchcock, J. H. (2011). Underlying agreements between quantitative and qualitative research: The short and tall of it all. *Human Resource Development Review*, *10*(4), 381. https://doi.org/10.1177/1534484311413867

Nevmerzhitskaya, J. J., Norvanto, E., & Virag, C. C. (2019). High impact cybersecurity capacity building. *E-Learning & Software for Education*, *2*, 306–312

Niemimaa, E., & Niemimaa, M. (2017). Information systems security policy implementation in practice: from best practices to situated practices. *European Journal of Information Systems, 26*(1), 1-20. https://doi.org/10.1057/s41303-016-0025-y

Maassen, M. A. (2018). Opportunities and risks of the agile software development management in the IT field. Case study: IT companies between 2009-2018. *Review of International Comparative Management / Revista de Management Comparat International*, *19*(3), 234–243. https://doi.org/10.24818/rmci.2018.3.234

Manworren, N., Letwat, J., & Daily, O. (2016). Why you should care about the target data breach. *Business Horizons*, *59*(3), 257-266. https://doi.org/10.1016/j.bushor.2016.01.002

Maria B., & Jason R.C. (2019). Developing cybersecurity education and awareness programmes for small- and medium-sized enterprises (SMEs). *Information & Computer Security (*3), 393. https://doi.org/10.1108/ics-07-2018-0080

Maynard, S. B., Tan, T., Ahmad, A., & Ruighaver, T. (2018). Towards a framework for strategic security context in information security governance. *Pacific Asia Journal of the Association for Information Systems*, *10*(4), 65. https://doi.org/10.17705/1pais.10403

Miranda, M. J. A. (2018). Enhancing cybersecurity awareness training: A Comprehensive phishing exercise approach. *International Management Review*, *14*(2), 5–10

McCrohan, K., Engel, K., & Harvey, J. (2010). Influence of awareness and training on cybersecurity. *Journal of Internet Commerce*, *9*(1), 23–41. https://doi.org/10.1080/15332861.2010.487415

McLane, P. (2018). Cyberattacks put every enterprise at risk: Techniques diversify as corporate adversaries get smarter. *Multichannel News* (15), 8

MediaPro. (2020). Employees would simply rather not with boring security awareness training, New Research Finds. Retrieved from https://www.mediapro.com/report-security-awareness-training-key element-security-culture

Merhi, M.I., & Midha, V. (2012). *The impact of training and social norms on information security compliance: a pilot study*. Thirty Third International Conference on Information Systems, Orlando

Mertler, C., & Vannatta-Reinhart, R. (2017). *Advanced and multivariate statistical methods* (6th ed.). New York, NY: Routledge

Mertler, C., & Vannatta, R. A. (2013). *Advanced and multivariate statistical methods.* Glendale, CA: Pyrczak Publishing

Mohamad Rashid, R., Zakaria, O., & Nabil Zulhemay, M. (2013). The relationship of information security knowledge (ISK) and human factors: Challenges and solution. *Journal of Theoretical & Applied information technology*, *57*(1), 67-75

Montesdioca, G. P. Z., & Maçada, A. C. G. (2015). Measuring user satisfaction with information security practices. *Computers & Security*, *48,* 267-280. https://doi.org/10.1016/j.cose.2014.10.015

Moody, G.D., & Siponen, M. (2013). Using the theory of interpersonal behavior to explain non-work-related personal use of the Internet at work. *Information and Management*, *50*(6), 322-335. https://doi.org/10.1016/j.im.2013.04.005

Mueller, M. (2017). Is cybersecurity eating internet governance? Causes and consequences of alternative framings. *Digital Policy, Regulation and Governance*, *19*(6), 415–428. https://doi.org/10.1108/dprg-05-2017-0025

Nam, T. (2019). Understanding the gap between perceived threats to and preparedness for cybersecurity. *Technology in Society, 58,*101122. https://doi.org/10.1016/j.techsoc.2019.03.005

Nasir, A., Arshah, R., & Ab Hamid, M. (2017). *Information security policy compliance behavior based on comprehensive dimensions of information security culture*: *A conceptual framework*. Proceedings of the International Conference on Information System and Data Mining.56-60. ACM. https://doi.org/10.1145/3077584.3077593

O'Driscoll, A. (2018). Terrifying cybercrime and cybersecurity statistics & trends. Retrieved from https://www.comparitech.com/vpn/cybersecurity-cyber-crime-statistics-facts-trends

Oravec, J., A. (2017). Kill switches, remote deletion, and intelligent agents: Framing everyday household cybersecurity in the internet of things. *Technology in Society*, *51*, 189–198. https://doi.org/10.1016/j.techsoc.2017.09.004

Organization of American States (OAS), Inter-American development bank cybersecurity report. (2016). Cybersecurity: Are we ready in Latin America and the Caribbean? Retrieved from https://www.sbs.ox.ac.uk/cybersecurity-capacity

Organization of American States (OAS). (2018). Critical infrastructure protection in Latin America and the Caribbean (OAS-Microsoft, 2018). Retrieved from http://www.oas.org/en/sms/cicte/prog-cybersecurity.asp

Paek, S. Y., & Nalla, M. K. (2015). The relationship between receiving phishing attempt and identity theft victimization in South Korea. *International Journal of Law, Crime and Justice*, *43*(4), 626-642. https://doi.org/10.1016/j.ijlcj.2015.02.003

Pálsdóttir, A. (2013). *Theory in Information Behaviour research*. [eBook edition] Sheffield, UK

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q). *Computers and Security*, *4*, 165-176. https://doi.org/10.1016/j.cose.2013.12.003

Posey, C., Roberts, T. L., & Lowry, P. B. (2015). The impact of organizational commitment on insiders motivation to protect organizational information assets. *Journal of Management Information Systems*, *32*(4), 179–214. https://doi.org/10.1016/s0378-7206(01)00115-x

Purkait, S., Kumar De, S., & Suar, D. (2014). An empirical investigation of the factors that influence internet user’s ability to correctly identify a phishing website. *Information Management & Computer Security*, *22*(3), 194-234. https://doi.org/10.1108/imcs-05-2013-0032

Purohit, B. & Singh, P. P. (2013). Data leakage analysis on cloud security. *International Journal of Engineering Research and Applications*, *3*(3), 1311-1316

Rahim, N. H. A., Hamid, S., Kiah, L. M., Shamshirband, S., & Furnell, S. (2015). A systematic review of approaches to assessing cybersecurity awareness. *Kybernetes*, *44*(4), 606-622. https://doi.org/10.1108/k-12-2014-0283

Ross, R., Dempsey, & K., Pillitteri, V. (2018). Assessing security requirements for controlled unclassified information. (NIST Special Publication 800-171A). Retrieved from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171A.pdf

Safa, N. S., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model in organizations. *Computers & Security*, *56*, 70-82. https://doi.org/10.1016/j.cose.2015.10.006

SANS (2019). Security awareness report: The rising era of awareness training. Retrieved from www.sans.org

Senthilkumar, K. & Easwaramoorthy, S. (2017). A Survey on cybersecurity awareness among college students in Tamil Nadu. IOP conference series. *Materials Science & Engineering*, *263*(4), 1. https://doi.org/10.1088/1757-899x/263/4/042043

Shillair, R., Cotton, S., Tsai, H.S., Alhabash, S., LaRose, R., & Rifon, N. (2015). Online safety begins with you and me: Convincing internet users to protect themselves. *Computers in Human Behavior*, (48), 199-207. https://doi.org/10.1016/j.chb.2015.01.046

Skarga-Bandurova, I., Ryazantsev, A., and Kiryushatova, K. (2016). An experience report on education and training programme in cybersecurity of critical infrastructures. *Information & Security*, *35*(2), 123–132. https://doi.org/10.11610/isij.3506

Solari, L. (2012). Globalization will make us all more different. *People and Strategy*, *35*(2), 30-35

Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *International Journal of Information Management*, 215-225. https://doi.org/10.1016/j.ijinfomgt.2015.11.009

Steinbart, P. J., Raschke, R. L., Gal, G., & Dilla, W. N. (2016). SECURQUAL: An instrument for evaluating the effectiveness of enterprise information security programs. *Journal of Information Systems*, *30*(1), 71-92. https://doi.org/10.2308/isys-51257

Stephen, H. (2011). Revisiting the Estonian cyberattacks: Digital threats and multinational responses. *Journal of Strategic Security*, *4*(2), 49–60. https://doi.org/10.5038/1944-0472.4.2.3

Stevens, T. (2018). Global cybersecurity: new directions in theory and methods. *Politics & Governance*, *6*(2), 1–4. https://doi.org/10.17645/pag.v6i2.1569

Tabachnick, B. G., & Fidell, L. S. (2013). *Using multivariate statistics*. Boston, MA: Pearson Education, Inc

Taitto, P., Nevmerzhitskay, A, J., & Virag, C. (2018). Using holistic approach to developing cybersecurity simulation environments. *ELearning & Software for Education*,*4*, 77–84. https://doi.org/10.48009/2_iis_2016_150-161

Tang, M., Li, M., & Zhang, T. (2016). The impacts of organizational culture on information security culture: A case study. *Information technology and Management*, *17*, 179-186. https://doi.org/10.1007/s10799-015-0252-2

Topa, I., & Karyda, M. (2015). *Identifying factors that influence employees' security behavior for enhancing ISP compliance*. Manhattan, New York: Springer International Publishing

Tsai, H-Y. S., Jiang, M., Alhabash, S., LaRose, R., Rifon, N. J., Cotten, S. R. (2016). Understanding online safety behaviors: A protection motivation theory perspective. *Computers & Security, 59*, 138-150. https://doi.org/10.1016/j.cose.2016.02.009

Udroiu, A. M. (2018). Implementing the cybersecurity awareness program using e-Learning platform. *ELearning & Software for Education*, *4*(43), 101–104

United States Securities and Exchange Commission [SEC]. (2015). *The need for greater focus on the cybersecurity challenges facing small and midsize businesses.* Washington, DC. Retrieved from https://www.sec.gov/news

Valiente Jr., C. (2017). Addressing malware WITH cybersecurity awareness. *ISSA Journal*, *15*(10), 16–22.

Veiga, A.D. (2016). A cybersecurity culture research philosophy and approach to develop a valid and reliable measuring instrument. 2016 SAI Computing Conference (SAI), SAI Computing Conference (SAI), 2016, 1006. https://doi.org/10.1109/sai.2016.7556102

Vitunskaite, M., He, Y., Brandstetter, T., & Janicke, H. (2019). Smart cities and cybersecurity: Are we there yet? A comparative study on the role of standards, third party risk management and security ownership. *Computers & Security*, 83, 313–33. https://doi.org/10.1016/j.cose.2019.02.009

Vogel, R. (2016). Closing the cybersecurity skills gap. *Salus Journal*, *4*(2), 32–46

VonSolms, R., & VanNiekerk, J. (2013). From information security to cyber security. *Computers & Security*, *38*, 97-102. https://doi.org/10.1016/j.cose.2013.04.004

Wall, J., & Buche, M. (2017). To fear or not to fear? A critical review and analysis of fear appeals in the information security context. *Communications of the Association for Information Systems, 41*(13), 277–300. https://doi.org/10.17705/1cais.04113

Wallden, P., & Kashefi, E. (2019). cybersecurity in the quantum era. *Communications of the ACM*, *62*(4), 120–129. https://doi.org/10.1145/3241037

Warkentin, M., & Orgeron, C. (2020). Using the security triad to assess blockchain technology in public sector applications. *International Journal of Information Management, 52,* 102090. https://doi.org/10.1016/j.ijinfomgt.2020.102090

Warner, R. M. (2013). *Applied Statistics: From Bivariate Through Multivariate Techniques.* (2nd ed.). Thousand Oaks, CA: SAGE Publications

Wasserman, E., & Migdal, R. (2019). Professional development: Differences in Teachers' attitudes in online and traditional training courses. *Online Learning*, *23*(1), 132–143. https://doi.org/10.24059/olj.v23i1.1299

Webb, J., Ahmad, A., Maynard, S. B., & Shanks, G. (2014). A situation awareness model for information security risk management. *Computers & Security, 44,* 1-15, https://doi.org/10.1016/j.cose.2014.04.005

Weishaupl, E., Yasasin, E., & Schryen, G. (2018). Information security investments: An exploratory multiple case study on decision-making, evaluation and learning. *Computers & Security*. *77,* 807-823. https://doi.org/10.1016/j.cose.2018.02.001

Wilding, N. (2016). Cyber resilience: How important is your reputation? How effective are your people? *Business Information Review*, *33*, 94-99. https://doi.org/10.1177/0266382116650299

Willan, M. M. (2016). Research approaches for higher education students: A personal experience. *BCES Conference Proceedings*, *14*, 247-254

Willison, R., & Warkentin, M. (2013). Beyond Deterrence: An expanded view of employee computer abuse. *MIS Quarterly*, *37*(1), 1-20. https://doi.org/10.25300/misq/2013/37.1.01

Wood, R., & Bandura, A. (1989). Social cognitive theory of organizational management. *Academy of Management Review*, *14*(3), 361–384. https://doi.org/10.5465/amr.1989.4279067

Yoo, C. W., Sanders, G. L., & Cerveny, R. P. (2018). Exploring the influence of flow and psychological ownership on security education, training and awareness effectiveness and security compliance. *Decision Support Systems*, *108*(02), 107–118. https://doi.org/10.1016/j.dss.2018.02.009

Zahid, E., & Shabbir, J. (2018). Estimation of population mean in the presence of measurement error and non response under stratified random sampling. *PLoS ONE*, *13*(2). https://doi.org/10.1371/journal.pone.0191572

Zak, M. & Ware, J. A. (2020). Cloud based distributed denial of service Alleviation system. *Annals of Emerging Technologies in Computing*, *4*(1), 44–53. https://doi.org/10.33166/aetic.2020.01.005

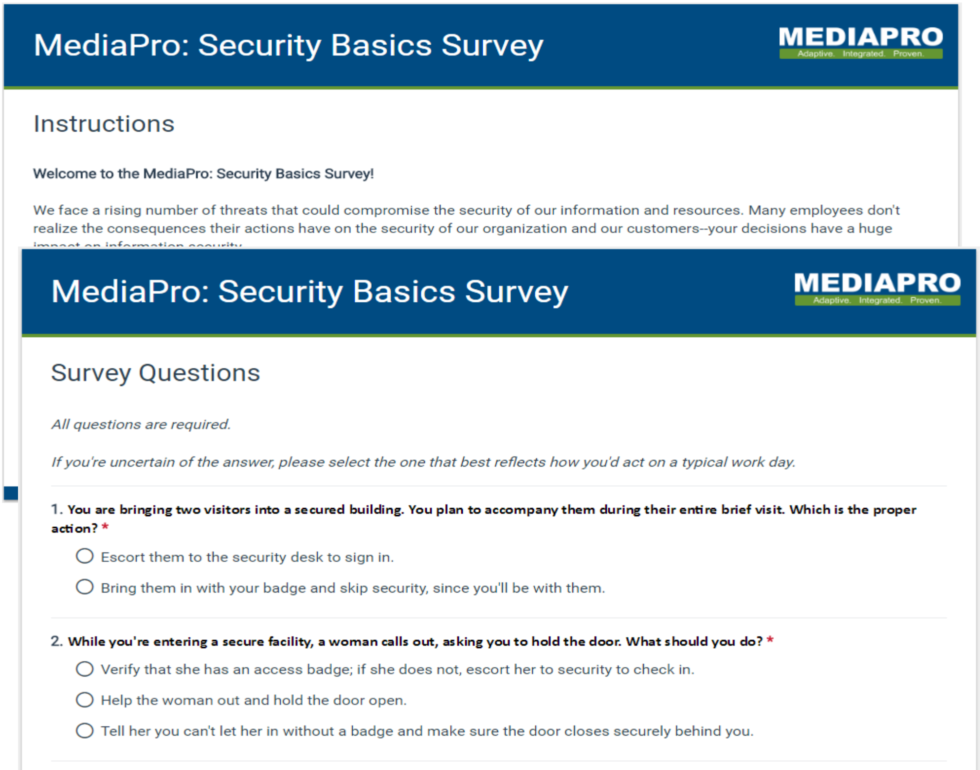
Zhu, S., Gupta, A., Paradice, D., & Cegielski, C. (2018). Understanding the impact of immersion and authenticity on satisfaction behavior in learning analytics tasks. *Information Systems Frontiers*, 1–24. https://doi.org/10.1007/s10796-018-9865-4

Appendix A: Risk Assessment Questionnaire

Risk Assessment

MEDIAPRO

Adaptive. Integrated. Proven.



MediaPro: Security Basics Survey

Instructions

Welcome to the MediaPro: Security Basics Survey!

We face a rising number of threats that could compromise the security of our information and resources. Many employees don't realize the consequences their actions have on the security of our organization and our customers--your decisions have a huge impact on information security.

MediaPro: Security Basics Survey

Survey Questions

All questions are required.

If you're uncertain of the answer, please select the one that best reflects how you'd act on a typical work day.

1. **You are bringing two visitors into a secured building. You plan to accompany them during their entire brief visit. Which is the proper action?** *

○ Escort them to the security desk to sign in.

○ Bring them in with your badge and skip security, since you'll be with them.

2. **While you're entering a secure facility, a woman calls out, asking you to hold the door. What should you do?** *

○ Verify that she has an access badge; if she does not, escort her to security to check in.

○ Help the woman out and hold the door open.

○ Tell her you can't let her in without a badge and make sure the door closes securely behind you.

Cybersecurity Awareness and Knowledge

Introduction

Welcome to the Cybersecurity Training

We face a rising number of threats that could compromise the security of our information and resources. Many employees don't realize the consequences their actions have on the security of our organization and our customers--your decisions have a huge impact on information security.

Thank you for agreeing to take part in this important Questionnaire designed to help identify and assess knowledge about security risks in order to target improvements within the organization. This Questionnaire takes about 10 minutes to complete, and must be finished in one session.

Physical Security

Your printers and fax machines sit in an area used by many people, including visitors. Which of the following is a best practice?

- ○ Keep a tray by each machine for faxes and printouts to be stacked upside-down until retrieval.
- ○ Retrieve documents immediately.
- ○ Have an employee collect and distribute incoming faxes and printouts at least hourly.

Safe Computing

Which of the following is the most secure password?

- ○ P@55w0rd123
- ○ password 123
- ○ pass123WORD
- ○ psswrd1234

Which of the following is the best advice about passwords?

- ○ Share your network password only with those you trust implicitly.
- ○ Create strong passwords that are difficult to guess.
- ○ Use the same password for work and home accounts; that makes them easier to remember.
- ○ Write down your passwords so you don't forget them…but keep them out of sight.

Which of the following is NOT a best practice for safe computing?

- ○ Keeping security software running
- ○ Keeping security software up to date
- ○ Downloading software that can help make your work more efficient
- ○ Downloading software only approved by your IT department

Which of the following is NOT a best practice for securing your computer?

- ○ Manually locking your computer when you leave your desk
- ○ Setting your screensaver to appear after five minutes of inactivity and requiring a password to unlock the screen
- ○ Securing your laptop if you leave it at work
- ○ Keeping your computer logged on to the network at all times

Phishing

Which of the following could indicate a phishing attempt in an e-mail message, even if logos and images make the message appear to be from a trusted source?

- ○ A request for you to reply at your leisure
- ○ An urgent problem to which you must respond quickly
- ○ No typos or grammatical errors
- ○ A statement that the enclosed offer will end next month

Which of the following could indicate a phishing attempt in an e-mail message, even if logos and images make the message appear to be from a trusted source?

- ○ A request to supply personal information
- ○ The message is addressed to you by name
- ○ No typos or grammatical errors
- ○ The message contains the signature and title of the sender

Protecting and Handling Data

Which is the most secure way to transmit a document with sensitive information to a client who is requesting it?

- ○ Attaching the unencrypted file to an e-mail message
- ○ Posting the file to a public FTP site
- ○ Posting the file to a secure FTP site set up for another client, and giving the client the password to use just this one time
- ○ Posting the file to a secure FTP site set up for this client to access with a password

Which is the most secure way to send a document attached to an e-mail message?

- ○ Encrypt the document and attach it to a message using your personal e-mail account.
- ○ Attach the unencrypted document to a message using your work e-mail account.
- ○ Encrypt the document and attach it to a message using your work e-mail account.
- ○ Attach the unencrypted document to a message using your personal e-

mail account.

Safe Remote and Mobile Computing

Which is the safest place to store business e-mails and contacts?

- ○ On your mobile device
- ○ On our network server

Which of the following could be risky to store on the mobile device you use for work?

- ○ Personal photos
- ○ List of upcoming birthdays
- ○ Links to our company and insurance provider's websites
- ○ Passwords and password hints

Privacy and Personal Information

Which of the following is the best definition of "privacy"?

- ○ An individual's expectation that their personal information is used at the company's discretion.
- ○ An individual's expectation that their personal information may be disclosed to unauthorized parties.
- ○ An individual's expectation that their personal information is used in limited ways and protected from disclosure to unauthorized parties.

Privacy applies to which of the following?

- ○ Personal information
- ○ Shareholder data
- ○ Employee data
- ○ All of the above

Which of the following is considered non-personal information—information that does not require safeguards?

- ○ Social Security number
- ○ Driver's License number
- ○ Account number
- ○ Name and breed of household pet
- ○ First and last name with address

Which of the following statements is based on the privacy principle of choice?

- ○ We are allowed to take unrestricted liberties with customer and employee data.
- ○ We give employees and customers the choice to have their data

protected from loss or theft.

○ We offer customers and employees the opportunity to control how we use their personal information and who we share it with.
○ We give employees the choice to share customer information with third parties as an incentive to close a deal.

You are tasked with calling customers to make sure their data is up to date and accurate. Which privacy principle is involved in this scenario?

○ Access
○ Security
○ Data Integrity
○ Enforcement

Privacy Responsibilities

You have a responsibility to follow our privacy policies whether or not your job duties include handling personal information.

○ True
○ False

Who is responsible for following privacy policies and safeguarding personal and confidential information?

○ Only managers and supervisors
○ Only top management
○ Every person we hire, including you
○ Only employees who handle personal and confidential information

Catie accidently leaks customer information on a social media site. What is a possible consequence of her actions?

○ Shares in the company skyrocket.
○ Loss of customer trust.
○ The company is praised for being transparent.
○ There are no consequences, sometimes these things just happen.

John's responsibilities include collecting and managing customer data. In his daily work, John should protect personal information from which of the following?

○ Destruction
○ Access
○ Loss
○ All of the above

To ensure that you are handling personal information properly, you should:

○ Use your best judgement when handling personal information.
○ Review and follow our privacy policies and procedures.
○ Access and monitor all personal information at all times.

Zoe works the night shift in the office doing janitorial work. Should she worry about protecting personal information at his job?

○ No, Zoe does not work with personal information and therefore does not need to protect it.
○ Yes, it is every employee's responsibility whether they work directly with personal information or not.

Global Privacy Laws

There is one single law that governs the way all countries must handle and protect personal information.

○ True
○ False

Privacy laws vary from country to country, as do penalties for violations.

○ True
○ False

Demographic Information Questions

What is your age in years from your last birthday? _________

What is your location of residence?

☐ City
☐ Rural
☐ Urban

What is your gender?

☐ Male
☐ Female

What is your rating of your level of internet access?

☐ Excellent
☐ Good
☐ Fair
☐ Poor

How long have you worked for [organization]?

- ○ Less than 1 year
- ○ 1 – 2 years
- ○ 3 – 5 years
- ○ 6 – 10 years
- ○ Over 10 years

Which of the following information do you collect, access, and/or store as part of your job responsibilities? *Select all that apply.*

- □ Social Security Numbers (SSNs)
- □ Credit card information
- □ Bank account information
- □ Medical or health information
- □ Full names, physical and e-mail addresses, phone numbers
- □ Intellectual property
- □ Employee information
- □ None of the above