2020

Strategies Universities' and Colleges' IT Leaders Use to Prevent Malware Attacks

Felix Agyei
Walden University

Walden University

College of Management and Technology

This is to certify that the doctoral study by

Felix Agyei

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. Donald Carpenter, Committee Chairperson, Information Technology Faculty
Dr. Bob Duhainy, Committee Member, Information Technology Faculty
Dr. Gail Miles, University Reviewer, Information Technology Faculty

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

Walden University
2020

Abstract

Strategies Universities' and Colleges' IT Leaders Use to Prevent Malware Attacks

by

Felix Agyei

MS, Saint Joseph's University, 2016

BS, Kwame Nkrumah University of Science and Technology, 2008

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Information Technology

Walden University

December 2020

Abstract

Information systems at universities and colleges are not exempt from the threat of malware. Preventing and mitigating malware attacks is important to universities’ and colleges’ IT leaders to protect sensitive data confidentiality. Grounded in general system theory, the purpose of this exploratory multiple case study was to explore strategies universities’ and colleges’ information technology (IT) leaders use to prevent and mitigate malware attacks. Participants consisted of 6 IT leaders from 3 universities and colleges in Southern California responsible for preventing and mitigating malware attacks. Data were collected through semistructured video teleconferences and 7 organizational documents. Three significant themes emerged through thematic analysis: personnel issues, security planning, and security management practices. A key recommendation is for IT leaders to implement a training and awareness program to address personnel issues. The implications for positive social change include IT leaders potential to secure students’, parents’, and faculty's confidential information, thereby reducing IT protection costs and preventing identity theft.

Strategies Universities’ and Colleges’ IT Leaders Use to Prevent Malware Attacks

by

Felix Agyei

MS, Saint Joseph’s University, 2016

BS, Kwame Nkrumah University of Science and Technology, 2008

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Information Technology

Walden University

December 2020

Dedication

I would like to dedicate this study to my mother, Nana Afua Anane. If it wasn’t for her strenuous effort toward my education and sustenance, I doubt I would ever have graduated from college. Also, to my fiancée for her unwavering support throughout this program. I am honestly appreciative to have a lady who keeps pushing me to achieve the greatest goals in my life. I have come this far because of the support I receive from family and friends like Mr. Eric Asare, Dr. Osei and Family, and Dr. Yaw Osei Adutwum.

Acknowledgments

I would like to acknowledge the indelible support I received from my chair, Dr. Donald Carpenter, and my second committee member, Dr. Bob Duhainy. With their support, guidance, and consistency, I was able to complete this milestone in my life. Although there were challenges, their guidance created enough assurance throughout this study.

Table of Contents

List of Tables

Section 1: Foundation of the Study

Background of the Problem

Malware attacks are on the rise in all industrial settings within the United States and the world at large (Curry & Drage, 2017). Universities and colleges are no exception when it comes to malware attacks, although some stringent strategies have been adopted to combat this menace **(**Koebel, 2017). Some IT leaders in universities and colleges lack strategies to prevent malware attacks in their network (Kvon et al., 2018). The collaborative nature and academic values of colleges and universities, coupled with the heterogeneity of gathered confidential information, make it a challenge to fight against malware attacks (Borgman, 2018).

Existing research on this topic formed the foundation for the conduct of this study. Misenheimer (2016a) examined computer and IT security training practices in universities and colleges with the intent to furnish IT leaders with needed information to combat information security threats. Some major findings of Misenheimer's study addressed the lack of comprehensive mitigation and prevention strategies for IT leaders, staff, and students in the area of IT security. Another significant finding of Misenheimer's study was the absence of training geared toward malware prevention in universities and colleges. Drawing on this, I developed a main objective in this study of exploring strategies that IT leaders in universities and colleges used to prevent malware attacks.

Problem Statement

Malware attacks remain a serious problem for higher education information technology leaders (Joshi & Singh, 2017). The United States Department of Justice (DOJ, 2018) reported $3.4 billion in losses associated with 144 universities in malware and other hacking-related attacks in 2017. Sixty-four percent of universities and colleges reported the absence of malware control strategies in their network. Colleges and universities experienced 13% of all malware attacks in the United States in 2016, ranking first among government, healthcare, energy, retail, and finance industries (Joshi & Singh, 2017). The general IT problem is that IT leaders of universities are faced with the challenge of safeguarding information systems from malware attacks. The specific IT problem is that some colleges’ and universities’ IT leaders lack strategies to protect information systems from malware attacks.

Purpose Statement

The purpose of this qualitative multiple case study was to explore strategies that colleges’ and universities’ IT leaders use to prevent and mitigate malware attacks to information systems. Data were collected from IT managers and chief information officers (CIOs) of three colleges and universities in Southern California who had strategies to protect information systems from malware attacks. The findings of this study may contribute to positive social change by reducing risks to students’ and parents’ private information as a result of malware attacks.

Nature of the Study

A multiple qualitative case study was utilized in this research with semistructured interviews to answer the research question. The qualitative method facilitates a deeper understanding of a study’s focus (Korstjens & Moser, 2017a). Because I intended to understand at a deep level the strategies that college and university IT leaders use to protect information systems from malware attacks, a qualitative method was appropriate for this study. Quantitative research, by contrast, uses mathematical models, theories, and hypotheses to gain insight into a phenomenon of interest (Rahi, 2017). A quantitative research methodology was not relevant to this study because the research did not utilize mathematical models. The mixed methodology combines the capabilities of both qualitative and quantitative research approaches to answer a research question (Rahi, 2017). Because this study did not involve a quantitative component, a mixed approach was not applicable in this context.

There are five qualitative research designs: case study, phenomenological study, grounded theory, narrative, and ethnographic study (Korstjens & Moser, 2017b). The yardstick for differentiating each qualitative research design type is tied into the study objective (Rahi, 2017). According to Roller and Lavrakas (2018), case study research design is a popular choice for gaining a deeper understanding of an event through multiple types of data. Case study research design was appropriate for this study, given that my objective was to explore strategies that IT leaders use to prevent malware attacks in universities and colleges. A multiple case study gives much stronger and more reliable findings, which can be verified by comparing data from varied sources (Ben-Hador, 2016). I chose multiple case study for this study because it allowed me to reach strong, reliable research findings. Ethnographic research design involves understanding a culture, ethnic group, or sect of people (Schadler, 2019). Because my research did not involve gaining an understanding of the cultural practices of a particular sect of people, an ethnographic research design was not appropriate. Narrative research design, as described by Grysman and Lodi-Smith (2019), weaves together a sequence of events from one or multiple participants to form a coherent story. For this study, I did not need to discuss the life events and experiences of an individual; therefore, narrative research design was not applicable. Thompson (2018) described phenomenological design as appropriate for studying the lived experiences of an individual as they relate to a unique phenomenon. The study did not involve gaining detailed comprehension of an event; hence, phenomenological design was not applicable.

Research Question

What strategies do IT leaders in colleges and universities use to prevent malware attacks to information systems?

Interview Questions

1. Do you personally have training in malware attacks? If not, why not? If so, how effective has the training been?
2. What strategies have been employed to protect the institution’s information systems from malware attacks?
3. What strategies failed to protect the institution’s information systems from malware attacks?
4. Are there both internal and external attacks in this institution? If so, which are most destructive?
5. Does this organization provide an adequate budget to address malware attacks?

6. Are staff equipped with the needed skills to address malware attacks in this institution?
7. What are the biggest sources of malware in this institution?
8. What policies have you adopted in relation to dealing with malware attacks in this institution?
9. What additional information do you want to share in regard to strategies to prevent malware attacks in the university's or college's information systems?

Theoretical or Conceptual Framework

This qualitative study utilized general system theory (GST) as a conceptual framework. In his 1968 seminal book *General Systems Theory: Foundations, Development, and Applications*, von Bertalanffy explained a system as characterized by a miscellany of interrelated and interdependent components. Von Bertalanffy (1951) proposed a resemblance of structure common among biological organisms from the micro to the macro level, especially concerning cells, organizations, human beings, and the society as a whole. The theory involves an assumption that universal principles govern all systems, whether mental, biological, social, physical, or chemical. Proponents of GST assume that all systems are components of a larger whole and that they share some similarities in terms of structures and functions, independent of their respective domains (von Bertalanffy, 1951). Katz and Kahn (1969) extended GST to address three characteristics of every system—hierarchy, homeostasis, and purposiveness. The theory postulates the existence of models, laws, and principles that apply to general systems irrespective of their kind, mechanisms, and interactions between them (Katz & Kahn, 1969). The main objective of the theory is to provide grounds for the development of unifying principles geared toward the integration of various sciences, natural and social (Edmonds, 2017).

In terms of their structure and functionalities, systems can be viewed from the following perspectives: open systems, holistic view, goal directedness, and self-organizing. An open system exhibits persistent evolution through its interaction with the environment, which determines the survival of the system (von Bertalanffy, 1951). According to Edmonds (2017), von Bertalanffy (1968) described an open system as consisting of inputs, outputs, transformation processes, feedback, and consistent interaction with the external environment. The holistic view focuses on the mutual interaction of the individual parts of a system, which makes the whole bigger than the parts. Accordingly, coordination among the respective parts of the system augments the relationship of the parts that connect to form a whole. Schelbe, Randolph, Yelick, Cheatham, and Groton (2018) pinpointed higher education institutions as open systems with the respective attributes of inputs, outputs, transformation processes, feedback, and consistent interaction.

In the same vein, government regulatory, sociocultural, and political forces constitute the environment that shapes higher education institutions (Teece, 2018). Mania-Singer (2017) linked aspects of the education system with the input, output, feedback, and transformation elements of an open system. In this light, colleges and universities are regarded as social systems that consist of students, are goal oriented in nature, achieve objectives through some form of coordination, and interact with their external environment.

Similarly, higher education institutions are classified as an open system with interdependent and interacting components, alluding to the holistic trait of GST (Adkoli & Parija, 2019). Edmonds (2017) noted that knowing a section of a system facilitates knowledge about other parts of the system. Therefore, higher education institutions are exemplified as open systems, such that information about one institution can give similar information about others. Information management and compliance regulations remain an integral element of higher education systems and therefore align with this study exploring the strategies that IT leaders in universities use to safeguard or mitigate malware attacks (Adkoli & Parija, 2019). In that all universities are required to adhere to the same privacy and policy mandates, GST indicates that they need similar structures and functions to achieve this aim, and therefore similar strategies. Goal directedness addresses systems as goal-oriented entities that rely on environmental feedback to fulfill such goals (Adkoli & Parija, 2019). A system is considered closed if is unable to import and export energy concerning its environment. The existence of a system is proportional to the rate of energy import and export across its boundaries or with the ability to internally source new energy.

Definition of Terms

Malware: Malware is an umbrella term used to address any program or file designed with the motive of causing harm to computer users in the form of stealing confidential data and gaining unauthorized access to systems (Rrushi, 2016).

Data breach: A data breach is an accidental or planned disclosure of corporate, government, or personal confidential or otherwise sensitive information (e.g., personal health information, trade secrets, personally identifiable information, intellectual property, or social security numbers) in an unlawful manner to achieve financial or other benefits (Goode, Hoehle, Venkatesh, & Brown, 2017).

External threat: External threats are malicious operations affecting corporate institutions, government, or any other entities orchestrated by actors outside their jurisdiction with the intent to exploit security weaknesses though insider social manipulation or software bugs that emanate from outside the network firewall (Greenaway & Cruwys, 2019).

Internal threat: An internal threat is a security threat that originates from an institution and is mostly perpetrated by current and former employees, stakeholders, external contractors, and vendors in an unintentional or deliberate attempt to compromise sensitive information, thereby interrupting the delivery of information system services (Marcus, 2018).

Network vulnerability: Network vulnerability is an effect within a computer system that can be exploited by a cybercriminal or an attacker in order to perform illegal actions (Aytac, 2019).

Phishing: Phishing is the illegal practice of obtaining sensitive or confidential information, such as personally identifiable information, social security numbers, credit card numbers, and login credentials, from targets contacted through emails, phone calls, or text messages purporting to come from legitimate sources (Sarikaa & Paul, 2017).

Assumptions

Assumptions are factual aspects of research that are out of the control of the researcher yet play an indispensable role in a study (Armstrong & Kepler, 2018). In this study, I made three assumptions. The first assumption was that research participants would honestly respond to interview questions. To encourage honesty, participants' anonymity was established before conducting the interviews. The second assumption was that the data collected through semistructured interviews would be enough data to help answer the overarching research question. The third assumption was that the chosen sample was representative of the given population studied to generalize results—in this case, higher education institutions.

Limitations

Research limitations are potential constraints that are out of control of the researcher and hinder the transferability of study findings to other conditions (Velte & Stawinoga, 2017). I limited my study to universities and colleges in Southern California because I could not afford the resources necessary to travel outside the research setting to interview other subjects. In light of this limitation, I am providing my research findings as a springboard for future researchers to look into other populations given the evidence from my study. As stated by Rahman (2017), in addition to contributing to existing knowledge, study findings help other researchers perform follow-up studies to better understand a phenomenon of interest.

Delimitations

Delimitations are traits chosen by a researcher to set the boundaries of a study

(Spekle & Widener, 2018). Research participation was restricted to higher education institutions' IT leaders in Southern California. I utilized a semistructured interview instrument for data-gathering purposes in this study.

Significance of the Study

Contribution to Information Technology Practice

There has been an influx of less equipped information security professionals in higher education institutions and other sectors of the industry (Misenheimer, 2016b). Misenheimer (2016b) attributed the absence of highly qualified information system professionals in the IT industry partly to the unavailability of training resources. In light of this, findings of this study may contribute to the practice of IT by serving as a repository of information to inform the drafting of stringent strategies and policies to combat the threat to systems. The findings of the study may serve as an information resource to augment the training of upcoming IT security professionals or leaders. The need for such information is linked to an increasing shortage of information security professionals, which was projected to hit 1.5 million by the year 2020 (Furnell, Fischer, & Finch, 2017). The study findings may serve as a resource to IT professionals already in the field seeking to rekindle existing strategies and develop new ones. Similarly, professionals in IT organizations can benefit from the findings of this study in developing training materials for employees and high-level managers to eliminate obsolete and inefficient practices.

Implications for Social Change

Application of the results of this study may enhance the management of sensitive data in educational organizations, leading to the avoidance of revenue loss. Brown (2016) estimated an associated cost of $673,767 per information security breach occurrence. In this regard, employing effective strategies may save higher education institutions afterbreach remediation expenses as well as federal compliance violation costs. This may improve the provision of high-quality educational resources, which in the long run may benefit society at large. The adoption of security strategies may augment the secured delivery and protection of intellectual properties, thus addressing societal issues and concerns. The findings of this study may support universities and colleges in saving costs associated with an information security breach. Such cost savings may be passed onto students and university staff in the form of lower tuition fees and better conditions of service, respectively. The findings of this study may be beneficial to individuals by saving them from identity theft and its ramifications. Additionally, unnecessary costs and losses linked to data privacy breaches may be avoided or mitigated.

A Review of the Professional and Academic Literature

Overview

The purpose of this multiple qualitative case study was to explore strategies that colleges' and universities' IT leaders use to prevent and mitigate malware attacks to information systems. This review of the professional and academic literature addresses the nature of such strategies and ties this research to a conceptual framework. The literature review forms an integral part of the study with the main objective of critically analyzing and synthesizing various academic resources about the topic of study (Wine et al., 2017). A good literature review is a typology of articles and research materials about a study area, showing lapses and areas of misunderstanding while presenting grounds for further inquiry (Wine et al., 2017).

Resources for this literature review were identified in various online repositories. Eighty-eight references were used to facilitate crafting the content of this synthesis and analysis. Eighty-four of the 88 references were published within the last 5 years, forming 95.5% of the total references. All of the 88 references were peer reviewed, forming 100% of total references. There are 290 sources used in the entire document.

The strategy for searching literature was focused on using certain keywords to help narrow the search criteria. The following search words were employed: *data breach, network data breach, software bugs, data fraud, data espionage, cybercrime, personally identifiable information theft, information theft, compromised information, information security flaws, higher education, universities, colleges, data leak, network hacking, spear phishing, computer virus, malware, social engineering, intellectual property theft, information loss, denial of service attack, SQL injection, browser weakness, malicious software*, and *network vulnerabilities.* Using articles' International Standard Serial Number (ISSN) in combination with Ulrich's Periodicals Directory, I verified that they were peer reviewed. An article without an ISSN was verified with the journal's title in Ulrich's Periodicals. Scholarly electronic materials were identified through Google Scholar, ProQuest, IEEE Xplore Digital Libraries, and Elsevier.

The literature review is organized in the following sections: General Systems Theory, Application of General Systems Theory to Education Settings, Theories That Support General Systems Theory, Theories That Contrast With General Systems Theory, Comparison of Prior Studies That Used General Systems Theory, Information Security Breaches, Information Security Strategies, Evolution of Malware, and Malware Detection Strategies.

General System Theory

I used GST as the conceptual framework for this study. A system, in its encyclopedic conception, entails a multiplex of interacting constituents in collective relationships that augment an identification of a border-maintaining entity or procedure (Ohi, 2017). According to Edmonds (2017), the development of systems theory occurred during the post-World War II period through the works of Ludwig von Bertalanffy. Von Bertalanffy, in his 1968 seminal book *General Systems Theory: Foundations, Development, and Applications*, explained a system as characterized by a miscellany of interrelated and interdependent components. Von Bertalanffy's book emphasizes the commonality of principles in the structure and operations of systems of all types and sizes. Von Bertalanffy (1968) outlined an interdisciplinary science employed for universal applicability and shared etymology. The theory postulates the existence of models, laws, and principles that apply to systems in general, regardless of their kind, mechanisms, and interactions with other systems. The tenets of GST predict the universality of principles that govern all systems, whether mental, biological, social, physical, or chemical. In other words, GST involves an assumption that all systems are components of a larger whole and that they have similarities in terms of structures and functions, independent of their respective domains (von Bertalanffy, 1968).

Before the 1940s, the subjects of complexity, self-organization, connectionism, and adaptive systems, which fall within the tenets of GST, had already been explored (Grimes, 2017). In the field of cybernetics, complex systems using mathematics had been examined by Norbert Weiner, William Ross Ashby, John von Neumann, and Heinz von Foerster (Motloch, 2017). Neumann posited cellula automata and self-producing systems. Howard T. Odum at the same time contributed to GST through the development of language requisition depicting energetics and kinetics at any system scale (Motloch, 2017). According to Mahajan et al. (2019), Odum became known for the development of the energy systems language through the tenets of circuit language of electronics. This presupposes that many scholars were engulfed in the idea of system theory development before von Bertalanffy formulated his GST. Evidence to buttress this claim is the 1912 to 1917 Tectology of Alexander Bognadov (Corneanu, 2017). Tectology was used to denote a unification of all social, physical, and biological sciences by classifying them as systems of associations and by looking for the underpinnings of their organizational principles (Mahajan et al., 2019). Gaisina, Belonozhko, Artyukhov, Sultanova, and Dallakian (2017) regarded tectology as the precursor of systems theory and synergetics.

Continuing with this system thinking, von Bertalanffy came up with GST in his 1968 work. According to von Bertalanffy, there exists correspondence in relation to the principles that govern the performance of entities that are inherently and widely dissimilar. Another fundamental principle of GST, as remarked by von Bertalanffy, is that evidence for the existence of general systems properties is linked to the appearance of structural resemblances or isomorphism in different disciplines.

Von Bertalanffy’s (1968) general system view was based on several fundamental ideas. First, all phenomena are perceived as an interconnected web of associations among elements or systems. The second fundamental idea is the commonality of patterns or similarities among systems irrespective of their kind, which can foster an understanding of the behavior of complex phenomena. Von Bertalanffy theorized that regardless of the composition and the relationship that exist among system components, there are models, laws, and principles that apply to general systems as well as their subclasses, denoting the existence of universal principles of organization common among varied disciplines. Giudici, Reinmoeller, and Ravasi (2018) stated that the main objective of GST was to demonstrate the presence of similarities of the theoretical paradigms of the various disciplines and proceed to develop a gamut of theories as well as a gestalt in theoretical thinkings. Von Bertalanffy's GST explores the mechanisms of phenomena, the collaboration that exists among such components, as well as the relationships that systems have with their environment.

Numerous researchers have contributed to expounding the principles of GST. Gastil (1975) noted that knowledge about one section of a system creates a precondition for knowing something about another part. Gastil furthered his contribution to systems thinking by stating that systems can be either controlled or uncontrolled. According to Gastil, in controlled systems, reformation is applied in response to the sensed information. As Gastil explained, Kuhn refers to sensed information as the detector, selector, and effector. A detector element of a system is used to address information communication between systems. The selector element defines the rules used in decision making, and the effector encompasses how transactions are made within the system.

Gastil posited communication and transaction as the only forms of interaction that occur within a system. Communication is the exchange of information, while transaction involves the exchange of matter and energy. Gastil elaborated system inputs as information exchanged from the environment into the system, while output is used to describe the flow of information from the system to its external environment. Over the years, GST has been used in various industries. Kast and Rosenzweig (1972) extended GST to include social systems such as the corporate world, universities, and hospitals. Bridgen (2017) extended system thinking to universities and colleges by classifying them as open systems that exchange information with their environment.

The holistic view encompasses the arrangement and relationships of the components of a system that connect them into a whole (Bridgen, 2017). In essence, mutual collaboration of these components makes the whole of a system bigger than the individual parts. Von Bertalanffy (1951) posited that it is necessary to evaluate a system by observing it as a whole, rather than through individual assessment of its constituents. The holistic view stresses the eradication of problems within a system by focusing on the system as a whole and how the individual constituents contribute to creating that whole. In this light, Barca (2017) contended that individual assessment of related components of a system negatively impacts the performance and effectiveness of the system. In the field of data security, an assessment of individual components of the system instead of its entirety negatively affects the overall quality of the system (Hryshchuk & Yevseiev, 2016).

GST was selected as the conceptual framework for this study because it encourages a holistic approach to problem resolution and augments the discovery of strategies that IT leaders in universities and colleges use to prevent malware attacks. With its focus on purposiveness, GST may be used to understand higher education institutions as composed of interrelated subsystems working together to achieve a common objective within a volatile environment. In this light, GST was deemed more appropriate to this study compared to other theories.

Application of General Systems Theory to Education Settings

In higher education institutions, IT leaders can effectively address data security breaches by looking at the problem as a whole in relation to higher education institutions instead of performing individual assessments (Yilmaz & Yalman, 2016). Von Bertalanffy (1951) described an open system as one that sends information to and receives information from its environment. A key trait of an open system is the constant dynamic interaction of its components with its environment. Six traits are common to open systems—inputs, process transformation, feedback, outputs, feedback, and the environment. Four types of resources are received from the environment to foster the operation of a school system—human, information, financial, and physical resources (Shen, Gao, & Xia, 2017). The school transforms the collected inputs through the utilization of technology and administrative functions (Butler et al., 2018). According to Shen et al. (2017), the internal interaction between students, professors, and other administrative staff contributes to the transformational process of creating literate scholars for society, which addresses the output component of the open system. Feedback in this context is the control mechanism; the feedback that the school receives from the environment guides the system in correcting deficiencies related to output or input transformation processes (Klein, 2017). Federal regulations such as the Family Educational Rights and Privacy Act (FERPA), in addition to economic and social forces, create the environment where universities and colleges operate, contributing to an open system environment (Marek & Skrabut, 2017). Klein (2017) recognized higher education institutions as systems and therefore fits the constituent description of open systems, thus justifying the adoption of this theory.

Purposiveness is another attribute of systems, according to GST (von Bertalanffy, 1951). Purposiveness in this context addresses the main objective or goal of every system. Banathy (1991) stated that the main objective of higher education institutions is the provision of literate individuals to society. Higher educational institutions’ goals also extend to employee improvement, federal compliance, and the provision of a harmonious environment. The goals of universities and colleges institutions vary, but satisfies the system attribute of purposiveness.

Another striking attribute of systems is homeostasis, which implies a self-regulatory mechanism whereby a system uses feedback from the environment. As noted by Porvazník and Ljudvigová (2016), homeostasis is the consistent maintenance of balance between a system’s internal and external environments.

The preceding paragraphs of this study address the relationship between data breaches, GST, and the specific IT problem. De Simone (2019) defined a data breach as a planned or accidental disclosure of secured or sensitive information to an untrusted environment, leading to potential interruption of confidentiality, integrity, and accessibility of affected data. Within this definition, the principles of integrity, accessibility, and confidentiality are stressed. Confidential information in this context encompasses personally identifiable information (PII) such as names, social security numbers, health information, intellectual property, and financial information. Gwebu, Wang, and Wang (2018) estimated that data breaches remain one of the primary threats to organizations and society at large. Sen and Borle (2015) stated that the average costs per data breach to the targeted organization as well as affected individuals amount to approximately $5.9 million.

Prior to the digitalization of information in corporate, education, government, health, and other industrial settings, paper-based information and documents were often stolen or compromised. All industries face operational challenges without the incorporation of technological resources. Pieters (2017) described the indispensable role that information systems play in organizations, the corporate world, and society at large. These systems have become as essential as water and oxygen to daily life. However, information systems, as hubs for sensitive and confidential information, remain “gold” targets for data criminals. The Federal Bureau of Investigation (FBI) Internet Crime Complaint Center (IC3, 2018) has estimated that an average of 900 data breaches occur every year. According to an IC3 report, data breaches are prevalent among health, higher education, and corporate institutions, as well as in other industries and society at large.

Considering universities and colleges as open systems, data is one of the critical components which is an asset to the institution (Banathy, 1991). Information exchange to and from its environment is, without doubt, an important attribute of higher institutions.

Universities and colleges are known to be a repository of large data from students and employees. The National Center of Education Statistics estimates 19.9 million colleges and university enrollment for the 2018-19 academic year (NCES, 2018). The internal transformation processes of colleges and universities require the collection of students' personally identifiable information such as names, social security numbers, health records, credit card numbers, course grades, research materials, intellectual property, and other sensitive information. The sensitivity and confidentiality associated with data coupled with federal compliance regulations that universities and colleges remain an undeniable fact that information is a great asset to such institutions. To save universities and colleges the cost, reputation damages, and litigation ramifications associated with compromised sensitive information through malware attacks, IT leaders must be equipped with the right tools and effective strategies to prevent or nullify such occurrence. Therefore it is imperative to inquire into existing strategies IT leaders use to prevent malware attacks in universities and colleges.

For IT leaders to successfully address malware attacks in universities and colleges, a holistic approach needs to be adopted. As stated by von Bertalanffy (1951), all systems are gestalt, a whole, that cannot be separated into its component sections and each dismembered element is secluded, but instead one needs to try to see the whole in interplay with all its interconnected and separate sections. In this light, IT leaders in colleges and universities can successfully address malware attacks by holistically focusing on the problem instead of an independent assessment (Borgman, 2018)

Theories Supporting General Systems Theory

Various theories were considered in order to determine the most appropriate for my research to explore strategies IT leaders use to prevent malware attacks. However, one of the notable supporting theory is the action theory by Parsons in his 1937 work. According to Parsons' action theory, characterized by a system theoretical approach is focused on a distinction between things that happen to a person and things that result from the person's actions (Münch, 1982). The problem of volition remains central to action theory and attempts to inquire about the connection between intention and body motion. According to Craig (2019), it is not advisable to separate motives from actions. Münch (1982) stresses objectives, results, and ideals must be considered by social sciences when observing actions. Action theory posits an interwoven analysis of actions hand-in-hand with the voluntaristic foundation.

The general system theory in harmony with action theory fosters a holistic view of a system entity and its environment and not an exclusive assessment of its individual constituent. Both theories frown on an exclusive assessment of phenomenon constituents but augment a holistic approach to a complex system. The contrasting traits between the two theories are that action theory is limited in scope to social settings while general system theory applicability is universally inclined. Action theory was not considered for this study because of its assumption of a cognizant choice that remains instrumental in guiding individual behavior especially in the light of predicted outcomes. Craig (2019) explains action theory is more application in predicting human behavior taking into consideration volition. In this light, action theory was not considered in this study since I do not intend to study social behaviors in this study.

Grey system theory is another theory that was considered but was not utilized in this study. Grey system theory was coined by Deng in his 1982 work to connote an instance of a system with partly known and unknown information (Deng, 1982). The theory defines systems with no information as black while those with perfect information were tagged white—a depiction that rarely exists in the real world (Deng, 1982). Grey was deduced from the dispersed or partial knowledge that exists between the two extremes (. i.e. white and black). Information in this context pertains to structure, operation mechanism and behavior form the fundamental principle of the grey system theory. Wang, Wang, and Zhang (2020) claimed the grey system theory was adopted to bridge the gap between the social and natural sciences and is known to apply to disciplines. Since grey system theory deals with the known and unknown parameters of a system, it was not chosen for this study because all information pertaining to this study are available.

Theories Contrasting With General Systems Theory

The complex adaptive system (CAS) supports the notion that an understanding of the individual components or elements of a system does not imply an automatic comprehension of the entire system’s behavior (Hodiamont et al., 2019). According to Hodiamont et al. (2019), CAS challenged cause and effect assumptions and therefore perceive all systems as a dynamic process. In the same vein, Herrera-Restrepo and Triantis (2019) claimed CAS portrays an environment where the interactions and associations of system constituents simultaneously affect and are shaped by the system.

According to Johnson, Holness, Porter, and Hernandez (2018), the general characteristics of CAS hovers around self-similarity, self-organization, complexity, emergence, and adaptability in the event of perturbation.

The central idea of the complex adaptive system theory suggests the universe is composed of complex systems and that each system resorts to persistent environmental adaptation (Espinosa, Davis, Stock, & Monahan, 2019). The adoption of complex adaptive system theory required the corporate leaders to have the development of new skills and strategies in a volatile and complex environment deprived of an expectation of stability and predictability (Espinosa et al., 2019). In contrast, the general system theory perceives all systems as part of a whole and an understanding of its constituents contributes to a comprehension of the entire system. The two theories are similar on the grounds of a universal or bigger system with related components.

One of the attributes of complex adaptive system theory is the difficulty to understand or predict the functionality of the whole system based on gathered information about its constituents (Werder & Maedche, 2018). As opposed to complex adaptive system theory, the general system theory augments the identification of problems, trends as well as the relationship that exist among constituents leading to the prediction of the entire system behavior (Edmonds, 2017). Drawing from this, the general system theory is more appropriate for the conduct of this research compared to complex adaptive theory.

The dual-process theory gives an account of how ideas can originate in two varied ways or result from two varied processes. Wason and Evans in their 1974 work, suggested the dual-process theory (Bronstein, Pennycook, Joormann, Corlett, & Cannon, 2019). According to Koenigs (2018), tenets of the dual-process theory dichotomizes processes into heuristic and analytic types. In the heuristic processes, individuals choose between the most relevant information out of the irrelevant ones about a situation at hand. The analytic processes proceed with the heuristic stage using. During the analytic processes, judgment is made using the relevant information ascertained from the heuristic processes. A dual-process theory presents the premise of a cognitive interaction between intuitive and deliberate thinking. Ingold, Donni, and Lievens (2018) posit moral judgment is the result of two competing processes—fast automatic intuitive processes and slow deliberate-based processes. In contrast to general system theory, the dual-system theory is more applicable to cognitive thinking geared towards moral judgment. While the general system theory is more focused on understanding and solving complex problems. In this light, the general system was more applicable to this study because of the associated trait of solving complex problems relative to the dual-process theory.

Checkland in his 10-year research project posited the soft system methodology to deal with the inadequacies of the hard system thinking for solving complex organizational issues with a large social component (AlHarrasi, 2016). The fundamental principle of the soft system theory revolves around an analysis of complex problems with varied perceptions on the problem definition (Checkland, 2000). The soft system methodology plays a pivotal role in harmonizing the various perspectives about an organizational problem through effective discussions. With his soft system methodology, Checkland brought to light the lack of consensus between developers and users. While the general system theory is more inclined towards a holistic approach to viewing a system or problem, soft system methodology focuses on stimulating a collective approach to a complex problem with a heterogeneous group of people within an organization. Both theories are similar in terms of adoption for complex problem resolution but vary in concepts and applicability. Soft system methodology was not chosen for this study because is more focused on dealing with the social component of complex problems while general system theory holistically views a problem or system taking into consideration the respective components.

Comparison of Prior Studies That Used General Systems Theory

GST and social networks were adopted to explore the relationship between stakeholders of a district's central office and principals of an elementary school (Mania-Singer, 2017). Findings show a scanty relationship between the two study groups—inhibiting the transfer of knowledge and communication and in the long run affecting teaching and learning. My study population is focused on IT leaders in universities and colleges. Mania-Singer's study sought to draw a relationship between members of a school district and elementary school principals and therefore contrasts my study on this ground. Mania-Singer's study was not focused on malware in higher education, therefore, it serves as a distinguishing trait with my study. Universities and colleges in Southern California is the target of my study, contrasting Mania-Singer's public schools in the Midwest.

In the same discipline, Dhukaram, Sgouropoulou, Feldman, and Amini (2018) employed the general system theory and socio-technical systems thinking to showcase the complexities associated with higher education provision as well as to comprehend the education ecosystem. Dhukaram et al. adopted a multiple case study and GST to comprehend the interactions and relationships between the parties (people, processes, technology, and the organization) of interest in European universities. My research differs from Dhukaram et al. in terms of the study location and population. I chose the United States of America while Dhukaram et al. focused on the United Kingdom. The focus of my research is to explore the strategies IT leaders in Universities and colleges use to prevent malware attacks. Dhukaram et al. sought to understand higher education provision using the systems thinking approach.

In the healthcare field, McClain, Johnson-Moton, Larsen, Ellis, and Niederhoffer (2018) utilized GST to guide the process of investigating the innovative partnership between pharmaceutical industries and academia. McClain et al. work capture the partnership between pharmaceutical industries and higher education institutions. My study is more focused on preventive strategies against malware in higher universities and colleges.

The concept of structural coupling, an element of the general systems theory was employed to explain the nature of money laundering in a United Kingdom bank as coupled with the adopted approach (Demetis, 2018). The author contributes to knowledge geared towards the detection of money laundering in an organizational setting. Also, a system-oriented framework for monitoring money laundering is presented in the study. Demetis employed the general system theory to explore money laundering in United Kingdom banks. The focus of my study is to explore the strategies IT leaders in universities and colleges use to prevent malware attacks, therefore serves as the differentiating factor in this context.

Information Security Breaches

A data breach is a planned or accidental disclosure of secured or sensitive information to an untrusted environment leading to potential interruption of confidentiality, integrity, and accessibility of the affected data (De Simone, 2019). Information security breaches are one of the scourges of an organization responsible for collecting sensitive data from customers and other stakeholders and universities and colleges are not exempted (Feng & Wang, 2019). The reason is, information criminals either cyber or physical demand the new gold—sensitive data (Feng & Wang, 2019). Organizations in the health sector host terabytes of data composed of patients' names, social security numbers, health records, diseases diagnosis information, credit or financial data, phone numbers, addresses, and other employees' confidential information (Zeadally, Isaac, & Baig, 2016).

Universities and colleges are not exempted from hosting confidential information about students and faculty staff (Rajab & Eydgahi, 2019). Enrolled students' dates of birth, credit and debit card details, other financial information, health records information, grades, intellectual properties, and information about federal and employees' data are left into the care of higher education systems (Rajab & Eydgahi, 2019). Similarly, retail, manufacturing, service, and other industries carry information about customers, users, and society at large (Kaušpadienė, Ramanauskaitė, & Čenys, 2019). Kaušpadienė et al. (2019) claimed information thieves either target these industries because of the nature and sensitivity of collected data which can be capitalized on for financial gains. Amid industries and corporations hosting high in demand information data by criminals, they are also required to increasingly comply with federal and information security regulations such as the 1974 Privacy Act, Family Educational Rights and Privacy Act (FERPA), health insurance portability and accountability act (HIPAA) (Marek & Skrabut, 2017). Drawing from this, companies and other industrial institutions are not just required to announce information security breaches, but also pay fines for violations.

Information security breaches rank number one in terms of the critical IT issues affecting universities and colleges (Misenheimer, 2016a). The average cost per compromised data in higher education institutions is about $245 coupled with reputation damages (Misenheimer, 2016b). Universities and colleges are prime targets for cybercriminals because of the influx of data-rich and multiple access environments (Bongiovanni, 2019). The FBI's internet crime and complaint center in its 2018 report claimed higher education institutions as the number one affected payroll diversion scam, followed by healthcare and commercial airway transportation (IC3, 2018). In March 2018, 144 United States universities were hacked resulting in the loss of 31 terabytes of confidential data with $3.4 million value in intellectual property loss (Bowdich, 2018). Malicious links associated with spear-phishing were the main culprit of these attacks (Bowdich, 2018).

The higher education sector has suffered multiple data breaches over the past ten or more years, contributing to billions of financial losses (Bowdich, 2018). A 2012 cyber-attack on Oracle’s PeopleSoft system at the University of Nebraska, resulting in a compromise of 654,000 students and staff information ((Bowdich, 2018). Derouet (2016) in his work, estimated the number of higher education information breach attacks increased to 393. The number of data breaches in the first half of 2017, skyrocketed by 164% compared to the last half of 2016 (Smyth, 2017). Phishing, malware, and software vulnerabilities are some of the main contributing factors of most of the data breach incidents in schools (Hammouchi, Cherqi, Mezzour, Ghogho, & Koutbi, 2019). Hammouchi et al. reported software vulnerabilities as one of the main contributors of some of the notable breaches.

For decades universities and colleges have been a target for espionage activities for intellectual property theft (Cathcart, 2019). China resorts to a continuous hacking campaign targeting two dozen universities (Cathcart, 2019). Cathcart discussed the Massachusetts Institute of Technology, University of Washington, Penn State, South Korea’s Sahmyook University are some of the named victims of China’s espionage. Espionage activities are not limited to higher education institutions, but other industrial and organizational settings as noted by Cathcart.

Information Security Strategies

In a complex landscape of advancement in technology coupled with a dynamic and Web 2.0 environment, it has become more challenging to deal with its associated information security challenges (Cathcart, 2019). Mansfield-Devine (2016) confirms a daily increase in the intensity and complexity of digital security threats. The persistent and diverse nature of the threat landscape warrants the need for more dynamic measures to curb information security incidents (Feng & Wang, 2019). An increase in information security attacks over the years has resulted in compensated investment to mitigate this menace. Jeong, Lee, and Lim (2018) described a 2015 Gartner survey estimating $7.1 billion in information security expenses in 2014, forming a 7.9% increase from a year before. In 2015, information security investment recorded $76.9 billion, confirming the increasing need for firms to protect their sensitive information assets (Weishäupl, Yasasin, & Schryen, 2018). In the same vein, Home Depot in response to the Target data breaches massively invested in security infrastructure reformation to upgrade cash registers to accept chip-enabled cards (Manion, 2016). Jeong et al. stated FireEye spearheaded Sony’s aftermath data breach to assess damages and to revamp infrastructure. However, with the current complex and evolving security environment, an increase in security investment does not guarantee a corresponding development of formidable security infrastructure. To complement huge investments to mitigate or prevent against data security threats, organizations or industries must adopt effective strategies (Manion, 2016). Deducing from Horne, Maynard, and Ahmad (2017) discussions on information security strategies, proactiveness, clear direction, business alignment and intelligent decision making were some of the tenets of effective security strategies.

A virtual user information security strategy based on group intelligent computing contributes to developing a secured system (Tan & Yu, 2018). According to Tan and Yu (2018), the algorithmic model collects visitors' private information historical access data which augments in the creation of threshold settings leading to the effective protection of the user. Jensen, Dinger, Wright, and Thatcher (2017) presented strategies to mitigate phishing attacks using mindfulness techniques. They give an additional layer to the rule-based approach which fails to progressively improve resilience to attacks irrespective of the persistence of application. Jensen et al. (2017) postulated the mindfulness theory to create a novel training approach to complement organizations already using rule-based strategy. The mindfulness approach enlightens individuals as to how best they can dynamically allocate during message assessment (Jensen et al., 2017). This approach helped inform individuals of the best evaluation techniques to distinguish between suspicious messages and legitimate ones (Jensen et al., 2017).

There exist some strategies aimed at addressing security challenges on a computer network (Xiaobo, Ying, & Jinhua, 2019). Xiaobo et al. (2019) emphasized the need for a hard-to-crack password and user credentials to protect against unauthorized network access. They advocate the need for strong firewall protection against malicious intrusions onto the network. To enhance a strong information security campaign, Xiaobo et al. (2019) highlighted the role of anti-virus on computers and other mobile devices. According to Xiaobo et al., anti-virus software effectively identifies malignant applications to nullify their potency. An additional layer of protection to the network and information transmission in the form of public-key encryption technology is also stated. This layer protects the integrity of email communication and the transfer of sensitive information from unauthorized intrusion (Xiaobo et al., 2019).

The sensitization of employees and insiders about practices that threaten the credibility of confidential data also contribute to existing information security strategies knowledge (Choi, Martins, & Bernik, 2018). Choi et al. (2018) explored the understanding of organizational insiders and stakeholders about information security practices and how they tie such knowledge into strategic actions. The researchers addressed the role of organizational insiders—a group that plays a critical role in the prevention, response, and mitigation of data security and prevention. Choi et al. (2018) stated organizational mission statement, threat awareness creation, information security education, the existing relationship between employees, accountability, and training sets an enabling environment for the creation of effective information security strategies. Their strategy addresses information security threats emanating from the human error factors. Choi et al. (2018) argued employees' behavioral factors as the main culprit of information security threats rather than technical causes hence the need for user-related strategies to address that.

Evolution of Malware

Malware is an acronym for malicious software, which denotes any program created with the intent to perform malevolent activities in a system (Namanya, Awan, Disso, & Younas, 2019). Executables, binary shellcode, script, and firmware are some of the manifesting formats of malware (Namanya et al., 2019). The idea of computer virus is linked to John von Neumann in his 1949 work Theory and Organization of Complicated Automata where he postulates the ability of computer programs to reproduce itself (Whitson, 2017). A year after, Bell Labs created the Core Wars game, bringing to reality Neumann's ideas (Whitson, 2017). Creeper worm by Bob Thomas was the first self-replicating computer program crafted in the BBN technologies Lab in the 1970s

(Ochieng, Mwangi, & Ateya, 2019). In this light, Bob Thomas is credited with creating the first self-replicating computer program virus (Ochieng et al., 2019). After the creepy worm, the Wabbit computer virus became popular in 1974 (Ochieng et al., 2019). The Wabbit computer virus was created with the ability to crash systems through a significant reduction of performance. Eight years after the Wabbit computer virus, Elk Cloner after its 15-year-old creator surfaced. Elk Cloner operated by displaying a little proem on affected computers and proceeds to infiltrate all the hard drives and the chips (Touchette, 2016).

The term computer virus was coined by Fred Cohen in his 1986 Ph.D. thesis (Touchette, 2016). Cohen in his work defined computer viruses as any program with the ability to infect other programs by changing their composition to reflect a possibly an evolved version of itself (Touchette, 2016). From this simple and gentle beginnings, a massive and diabolic industry came to being. Nineteen-eighty-six witnessed the first virus to infect MS-DOS—the brain boot sector virus created by two Pakistani brothers to assess the vulnerabilities in their program (Alajlouni, 2017). In the same year, PC-Write one of the earliest trojans was created as a shareware program (Touchette, 2016). PC-Write trojan can erase all users' files once it gets into the system. Morris worm affected a significant amount of computers connected to ARPANET resulting in a disruption of the internet within 24 hours (Wei, Mao, Oberg, & Kastner, 2016). Robert Morris the creator of the malware was the first to be convicted under the 1986 Computer Fraud and Abuse Act (Wei et al., 2016).

The Michelangelo virus of 1991 also came into light with the ability to erase information from a computer hard drive on March 6th, the birthday of the famous renaissance artist (Kaur, 2016). Melissa virus of 1999 contributes to this historical menace as the first mass-emailed virus which utilized outlook address books from infected computer systems and emailed to 50 people simultaneously (Kaur, 2016). Malware significantly gained popularity in terms of number and infection rates between 2000 and 2010 (Leukfeldt, Kleemans, & Stol, 2017). Later in the years, there was a dramatic increase in malware toolkits including the famous Sony rootkit which has contributed to malware authors' orchestration of their evil intent (Leukfeldt et al., 2017). Crimeware kits which target websites also increased significantly leading to the compromise of most online platforms (Horner & Hyslip, 2017). SQL injections became a serious threat to perpetuating victims like IKEA (Horner & Hyslip, 2017).

ILOVEYOU worm gained popularity in 2000 spreading through email medium with the benign subject line "ILOVEYOU" (Touchette, 2016). An estimated 50 million computers were affected by this worm leading to the incapacitation of government and corporate email servers (Touchette, 2016). There were $ 5.5 billion globally recorded damages due to the explosion of "ILOVEYOU" malware (Touchette, 2016). In 2001, an email purporting to have the pictures of Anna Kournikova the beautiful female tennis player had inherent malicious malware infecting users who clicked on an email link (Guo, Cheng, & Kelley, 2016). As the years progressed, more advanced bad software came to light. This is evident by the advent of the SQL slammer worm which by that time was one of the fastest spreading worms of all time (Horner & Hyslip, 2017). Within ten minutes of its discovery, the SQL slammer worm affected nearly 75,000 computers.

According to Horner and Hyslip (2017), SQL slummer launched a denial of service attack which resulted in a global slowdown of internet traffic.

The Cabir virus surfaced in 2004 and is the first mobile virus, although there is scant documentation about the rendered damage after discovery (Martinelli, Marulli, & Mercaldo, 2017). Touchette (2016) stated Koobface virus surfaced in 2005 and remained one of the first instances of malware with the ability to infect personal computers and proceed to proliferate to social networking sites. Facebook, MySpace, Twitter and other related social media platforms were targeted by this malware (Sowmya & Chatterjee, 2018). Detected in November 2008, the Conficker worm targeted Microsoft operating systems through existing vulnerabilities (Ochieng et al., 2019). The sophisticated Conficker malware affected millions of government, businesses and home computers of about 190 countries tagged as one of the largest malware infections since 2003 (Ochieng et al., 2019). Conficker worm capitalizds on the inherent flaws in the Windows operating system to propagate while forming a botnet (Ochieng et al., 2019).

From 2010 to the present, the world has experienced significant growth in sophisticated malware (Hatfield, 2018). Fidler (2017) contended the past nine years have witnessed malware explosion in the form of organized crime, state-sponsored attacks, and crime groups. The proliferation of these malicious workgroups continued to evolve with advanced malware evasion techniques with the capability to outsmart existing anti-malware systems (Zhong & Gu, 2019). From 2010 to present, malicious software propagation took turn infiltrating factories, military systems as well as the rapid growth of monetization of the menace (Zhong & Gu, 2019). Stuxnet worm was released with the intent to attack Iran’s nuclear program with the ability to incapacitate both the hardware and software. To date, it remains one of the resource-intensive bits of malware ever created (Albahar, 2019). Albahar argued Stuxnet worm targeted SCADA systems and is responsible for causing a substantial amount of damage to Iran’s nuclear program (Albahar, 2019). The worm exclusively targets programmable logic controllers, that control the automation of electromechanical processes for separating nuclear materials (Moreira, Molina, Lázaro, Jacob, & Astarloa, 2016).

Twenty-eleven witnessed the release of the Zeus Trojan sometimes called Zbot and became one of the most successful fragments of botnets that affected millions of computers (Moreira et al., 2016). Black, Gondal, and Layton (2018) in their work stressed Zeus trojan is popular in the theft of banking or other financial information by man-in-the-browser keystroke logging and form grabbing. As evidenced in the malware evolution, Cryptolocker surfaced between 2013 and 2014 with a momentous global impact (Richardson & North, 2017). Backoff malware was launched in 2014 to compromise point-of-sale (POS) systems to steal credit card data from retail stores. Through remote desktop type applications, this malware is installed where the point of sales systems are configured (Zhong & Gu, 2019). According to Kurniawan and Riadi (2018), Cerber malware was one of the copious crypto-malware threats in 2016 infecting many enterprise personal computers (Kurniawan & Riadi, 2018).

To confirm the extensive impact of the malware menace, the famous WannaCry ransomware took the world by storm in 2017 (Mohurle & Patil, 2017). Adams (2018) emphasized the ransomware capitalized on vulnerabilities in Windows operating systems in Russia, China, UK, and the United States. Adams (2018) contended WannaCry ransomware locked users from their databases and demanded ransom payment or lose confidential information. Hundred and fifty countries and industries such as hospitals, banks, telecommunication companies, and warehouses were impacted by this bad software (Christensen & Liebetrau, 2019). Giving the trend of malware evolution, there are no signs of growth slow down and therefore, technology users must resort to more creative and advanced strategies to combat this menace. It is therefore imperative to study the strategies IT leaders in universities and colleges use to prevent malware attacks.

Malware Prevention Strategies

Malware activities on the web have assumed a progressive growth over the past decade (Chen, Su, Qiao, & Xin, 2018). Documentation and reports in both digital and print media attest to the evolvement of new and advanced vulnerabilities and attacks coupled with the rapidly growing economic incentive presupposes the need for more ingenious means of dealing with this menace (Joseph & Mukesh, 2018). To contribute to the prevention strategies Aurangzeb, Aleem, Iqbal, and Islam (2017) claimed to minimize the risk of infected devices and victimization, prevention remains the utmost priority in this instance. According to Aurangzeb et al., receivers of Microsoft Office attachments must desist from enabling macros which can serve as a conducive atmosphere for bad software.

More, spam and gateway filters are efficient ways to stop ransomware infestation (Shah, 2017). According to Zhong and Gu (2019), businesses, government, and other corporate or individual receivers of confidential emails must consider subscribing to email filtering services like the one by Symantec as an additional layer of security to their email security cloud. Chandrasekar and Priyatharsini (2018) posited, to enhance the capability of the email filtering services, the application must be configured to block attachments with .cmd, .hta, .rar, .wsf, .xlsm, .exe, .7z, .pif, .reg and .vbs from suspicious senders. System administrators must avoid giving more than enough system roles during normal system use--browsing online, opening applications, and other related tasks (Mao, Cai, Towsley, Feng, & Guan, 2017). The objective of this strategy is to limit malware attacks to the assigned system roles, therefore, restricting the extent of damages during malware attacks (Mao et al., 2017).

Most bad software capitalizes on vulnerabilities within applications (Sharma, Gandotra, Bansal, & Gupta, 2019). Therefore it is imperative for system administrators to perform routine updates to apply patches to applications (Sharma et al., 2019). Web-filtering applications must be updated to reflect the latest versions to reduce the attack ratio (Kuchta, Palikareva, & Cadar, 2018). Min et al. (2018) claimed information technology professionals should consider weekly data backups and restoration. According to Min et al. (2018), data backups and recovery exercises augment the retrieval of confidential information by going back in time before the malware attack without paying any ransom to the attackers. Database administrators must execute backups to a separate drive that must stay detached from the network (Mabunda, 2019). Kuchta et al. (2018) reasoned that downloaded software must be scanned for malicious code before executing and installation. To contribute to the discussion, Richardson and North (2017) recommended up-to-date anti-viruses must be installed with the latest patches and schedule routine system scanning must be adopted to help defeat malware to a greater extent.

Transition and Summary

The purpose of this multiple case study was to explore strategies IT leaders in universities and colleges use to prevent malware attacks. To establish a scholarly background for the conduct of this study, I resorted to an extensive review of literature coupled with a critical analysis of information related to the research topic. The literature review was categorized into themes to help readers grasp the amount of gathered information about the topic.

Section Two of this work focused on detailed information about the basis for utilizing multiple case study to explore strategies IT leaders use to prevent malware attacks. Other components of Section Two was dedicated to an extensive explanation of the role of the researcher, participants, population and sampling, data collection, and analysis. Section three of this study was dedicated to the presentation of findings, applications to professional practice, implications for social change, recommendations for action and further study, reflections, and a strong concluding statement.

Section 2: The Project

Purpose Statement

The purpose of this qualitative multiple case study was to explore strategies that colleges' and universities' IT leaders use to prevent and mitigate malware attacks to information systems. Data were collected from IT managers and CIOs of three colleges and universities in Southern California who had strategies to protect information systems from malware attacks. The findings of this study may contribute to positive social change by reducing the risk to students' and parents' private information as a result of malware attacks.

Role of the Researcher

In qualitative research, the researcher plays the role of the data collection instrument (Karagiozis, 2018). As such, I was the data collection instrument for this qualitative multiple case study. As stated by Clark and Vealé (2018), the researcher acts as a human instrument responsible for data gathering, coding, and analysis from study participants' interviews and questionnaires to discover emerging themes and concepts while adhering to research ethics and standards.

I have worked as a data and system analyst in a school district for the past 8 years. I drew from experiences with information security breaches, but I had no prior relationship with the study participants, and I conducted interviews using an interview protocol (Appendix C). I established trust through professionalism to encourage participants' cooperation.

The Belmont Report (National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research, 1978) describes the basic ethical principles that must form the foundation for the conduct of biomedical and behavioral research involving human subjects. The report also sets guidelines that should be observed to ensure the conduct of research within the stipulated principles. Respect for individuals, beneficence, and justice are the three main underlying principles of the Belmont Report. Friesen, Kearns, Redman, and Caplan (2017) discussed mandatory ethical compliance as a fair criteria for determining study inclusion and exclusion as well as equal distribution of research burdens and benefits. Researchers' efforts should be directed toward minimizing risks and maximizing benefits for study participants and society (Glenna, Hesse, Hossain, & Scott-Villiers, 2019). These ethical principles guided me in conducting this research in compliance with the tenets of the Belmont Report.

There are risks of bias in all aspects of qualitative research, especially concerning study questions, respondents, and the researcher (Galdas, 2017). To reduce bias in my research, I employed best practices for data gathering. I recorded detailed field notes to help capture study participants' true views to help deal with both researcher and participant bias. As Buetow (2019) explained, researchers should consider implementing effective mechanisms to reduce research bias to increase study findings' favorability. Spiers, Morse, Olson, Mayan, and Barrett (2018) claimed that knowing the sources of bias plays a significant role in bias detection and minimization.

To reduce bias, I replaced any questions that might imply "correct" answers with alternatives designed to capture study participants' views. As opined by Buetow (2019), replacing questions with implied "right" answers with ones that seek respondents' true points of view fosters the minimization of research bias. Additionally, I dealt with habituation bias by wording questions in varied ways with the objective of engaging study participants throughout the interview process. Jordan (2018) recommended continuously varying questions and using a conversational type of interviewing to increase participants' engagement and reduce habituation bias. I followed best practices in collecting data from study participants in this regard. Likewise, I sought more information from a range of sources, especially participants' response confirmations, to avoid having preconceived notions about questions.

I adopted a semistructured interview approach coupled with a face-to-face interview strategy during the data-gathering process of the study. Using the interview protocol (Appendix C) as a guide, I was cognizant of my body language to avoid triggering perceptions that might result in research bias. Additionally, I avoided having predetermined thoughts because of the environmental parameters. I maintained a neutral body composure, as well as avoided facial expression that might result in bias from the respondent. I asked questions without offering personal opinions, and in the process data responses were gathered devoid of having preconceived notion and interruptions.

An interview protocol can support a researcher in gaining in-depth knowledge from study participants (Mohajan, 2017). The composition of an interview protocol is not limited to interview questions but extends to the procedural level of conducting an interview process, including a script detailing the content of what is to be said before and after the interview exercise (Hamilton, Powell, & Brubacher, 2017). An interview protocol is an embodiment of the questions and issues to be explored during an interview process or exercise (Hamilton et al., 2017). To gain detailed perspectives from qualitative research participants, researchers use face-to-face interviewing. An interview protocol should contain an introduction to the interviewee to break the ice and to reveal the purpose of the interview exercise (Castillo-Montoya, 2016).

Participants

I selected study participants for this multiple case study based on their expertise and knowledge about malware prevention in universities and colleges. The sample size determination in this study was dependent on the data saturation level. As posited by Sim, Saunders, Waterfield, and Kingstone (2018) in their response to the sample size debate, the required number of research participants is dependent on data saturation level. According to Boddy (2016), the determination of the number of research participants needed to reach data saturation depends on multiple factors—the quality of data, the study's scope, the topic in context, the number of interviews per participant, the richness of data collected from each participant, and the qualitative method or study design utilized. Blaikie (2018) contributed to the discussion on sample size estimation by stating that sample size determination is contextual in nature and is partly reliant on the scientific paradigm that structures the inquiry.

Participants in this study were IT leaders in universities and colleges in Southern California with expertise in the adoption of strategies to prevent information security breaches. To fulfill the objectives of the study, participants were expected to meet a specific set of criteria. Martinez-Mesa, Gonzalez-Chica, Duquia, Bonamigo, and Bastos (2016) suggested that participants in a study should have knowledge and experience about the research topic. Given this, prior familiarity and experience with the topic of interest were considered in selecting study participants. The section of colleges and universities for this study was based on their adoption of information systems to support the performance of departmental or institutional functions leading to the management of confidential information. Each selected participant was expected to have 7 years or more of experience in the adoption and implementation of security strategies to prevent malware attacks in universities and colleges. IT leaders were selected for this research because of the critical role that these individuals play in the provisioning of IT infrastructure and services in universities and colleges.

Gaining access to the field and gaining access to informants are fundamental tasks in conducting research (Amundsen, Msoroka, & Findsen, 2017). These tasks involve securing entry to certain organizations to ascertain whether employees and other stakeholders may serve as suitable participants in a study. Amundsen et al. (2017) stressed the pivotal role that an organizational chart plays in gaining access to research informants. Drawing from this, before contacting eligible study participants, I familiarized myself with the institutions’ organizational charts to avoid breaching protocol and to smoothly reach the main gatekeepers. According to Amundsen et al., the known-sponsor approach is one of the most effective strategies to establish researchers’ credibility leading to institutional entry. The approach is focused on establishing a connection with the higher level body that exercises overall control over the setting of the study.

I contacted the respective gatekeepers or individuals in equivalent positions at the selected universities and colleges. After securing their agreement, I emailed them a permission letter granting me the right to conduct the research on their campus. The email that I sent to the CIOs can be found in Appendix A. Once I had their agreement, I communicated with the respective universities and college CIOs to obtain a list of eligible study participants. Each potential participant was emailed the informed consent form detailing the main objective of the study as well as the possible benefits to the higher education institution (i.e., the potential of the study to inform efforts to revamp information security strategies against malware attacks). As an additional layer to the selection process, all participants were required to sign and agree to all terms of the presented consent form before participating in the study.

To sustain the already established working relationship with research participants, the confidentiality and anonymity of gathered information were assured through the informed consent form. The relationship between researcher and participants is integral to the quality of research output (Newton, 2017). Identifying eligible participants and securing their consent to be part of the study exercise were among the first steps in starting a working relationship (Howard & Hammond, 2019). Trust is one of the core ingredients of a strong working relationship between researcher and participants (Rinehart, 2019). To establish trust and respect, which are preconditions of searching for truth, I interviewed all participants at their respective offices. I also avoided any facial or body gestures that might jeopardize the data-gathering effort and the study as a whole. Through negotiations, a researcher and participants can develop a clearer understanding of their expectations, building trust and respect throughout the research process.

Research Method and Design

Method

In this study, a qualitative research approach was adopted after a succinct investigation of the available research methods coupled with the research objectives. Three main types of research methods exist—qualitative, quantitative, and mixed methods (Kluge, Schüffler, Thim, Haase, & Gronau, 2019). The purpose of the study played a significant role in the selection of the most appropriate method for this research (Kluge et al., 2019). A qualitative research methodology is focused on gathering nonnumerical data, in contrast to a quantitative approach. In the words of Surmiak (2018), a qualitative approach is explorative in nature, geared toward the provision of insights into a problem and fostering the development of ideas toward the conduct of future quantitative research. Thompson (2018) argued that a qualitative approach is useful in the discovery of trends, ideas, and thoughts pertaining to a problem and in diving deep into a problem of interest. The purpose of this study was to explore the trends and qualities of the strategies that IT leaders in universities and colleges use to prevent malware attacks; therefore, a qualitative method was the most applicable approach.

Qualitative methodology is more applicable to instances where research is focused on gathering words or text-related data rather than metrics, with the aim of depth instead of breadth (Bleiker, Morgan-Trimmer, Knapp, & Hopkins, 2019). Bleiker et al. (2019) claimed that a researcher adopting a qualitative approach seeks to exhume the opinions, feelings, and ideas of study subjects in relation to a central problem. Because the objective of this study was not to ascertain the number of effective strategies that participants had but to discover existing strategies, I used a qualitative approach to help in answering the central research question. As expressed by Mohajan (2018), a qualitative methodology is appropriate for the discovery of thoughts, ideas, and opinions about a problem. Because the main purpose of this study was to explore strategies that IT leaders in universities and colleges use to prevent malware attacks, I chose a qualitative methodology.

The quantitative method is inclined toward gathering numerical data on a problem of interest with the objective of formulating facts and uncovering patterns (Murshed & Zhang, 2016). Because the purpose of my research was not focused on quantifying facts and figures in relation to the central research problem, a quantitative approach was not applicable. In the same vein, Baškarada and Koronios (2018) claimed that quantitative methodology applies to studies in which researchers have the objective of depicting a correlation between two more variables and drawing a conclusion about a cause-effect equation. Moreover, a quantitative research design is geared toward establishing a relationship between a dependent and independent variable within a population (Bloomfield & Fisher, 2019). Because my study did not involve establishing a correlation or drawing a conclusion based on a cause-and-effect relationship between variables, a quantitative research approach was not applicable.

The main objective of this study was to explore strategies that IT leaders in universities and colleges use to prevent malware attacks; therefore, quantitative research methodology was not consistent with the research objectives. The mixed research methodology uses elements of both quantitative and qualitative approaches to help researchers explore diverse views and uncover relationships that exist between the various layers of a research question (Reilly & Jones, 2017). Because this study did not involve a quantitative component, a mixed approach was not applicable in this context. The objective of this study was to gather rich and in-depth information about the central research question and not to gather data for statistical analysis; therefore, a quantitative approach was not adopted.

Research Design

I chose a multiple case study approach because it provided tools that fostered a deeper understanding of similar and contrasting strategies that university and college top-level IT leaders use to prevent malware attacks to information systems. *Qualitative research design* is an umbrella term used to describe a range of approaches and methods that vary considerably in terms of focus, the role of the researcher, assumptions, and the nature of gathered information (Spiers et al., 2018). Researchers mostly adopt three major types of qualitative research design—case study, ethnography, and phenomenology (Spiers et al., 2018). To help in answering the overarching research question, I selected a multiple case study approach. Zahle (2018) stated that multiple case study facilitates wide exploration of the research question while granting in-depth understanding of the phenomenon under study. Abellán (2019) contended that multiple case study design supports the generation of strong and reliable study findings. In the same vein, Tobi and Kampen (2018) implied that multiple case study is well suited to similar and conflicting results comparison. A researcher can, therefore, determine the credibility of the study findings through a multiple case study approach.

A phenomenological research design is used to describe human experiences in relation to a particular phenomenon (Cypress, 2018). According to Jamali (2018), phenomenological research design eliminates biases and preconceived notions relating to human experiences, feelings, and reactions to a particular condition. It creates an environment in which the researcher delves into the perceptions, views, feelings, and comprehension of individuals who have actually experienced or lived the situation under investigation. Richards (2018) wrote that a phenomenological study utilizes in-depth interviews of small samples and that researchers can generalize the perspectives of those who have experienced the phenomenon. A phenomenological research design was not appropriate for this study because the research was not focused on an inquiry into live human experiences.

Ethnographic research design is most suitable for a situation in which the researcher is interested in observing or interacting with study participants’ environment and culture (Korstjens & Moser, 2017a). Ethnographic research design entails the literal representation of a group of people, taking into consideration the specific social setting. Rhiannon and Hurrell (2016) discussed the integral role that the researcher plays in the context of forming part of the group under investigation. Ethnography augments documentation of cultural similarities and differences via empirical fieldwork. Also, ethnography aids scientific generalization about human behavior hand-in-hand with the operation of social and cultural systems (Lai, Pagh, & Zeng, 2019). An ethnographic design was not feasible for this study because my objective was to explore strategies that university and college top-level IT leaders use to prevent information security breaches through malware, not to study the cultural environment of participants. Further, this study did not involve an investigation into a cultural or ethnic group; hence, ethnographic design was not applicable in this context.

Data saturation is commonly perceived as the point in the research process where no additional or new information is revealed in the data analysis and notifies the researcher a need to cease data collection (Hancock, Amankwaa, Revell, & Mueller, 2016). At this stage of the study, a researcher is assured further data collection will yield similar results that confirm and emerging themes and conclusions or findings (Hancock et al., 2016). Fusch, Fusch, and Ness (2018), in their work, discussed data triangulation as using multiple sources for the data collection on a research topic. According to Fusch et al., there is a direct link between data saturation and triangulation claiming one ensures the other. In other words, they argue that data triangulation is a method to get to data saturation (Fusch et al., 2018). To reach data saturation, I utilized other forms of documents related to the topic in addition to a multiple case study approach. To attain data saturation, I interviewed at least two participants in one university. If the second one presents new information, a third person in the university was interviewed. More people were added until no new information emerged. More, if second and third universities presented new information, I included a fourth university until no new information emerges.

Population and Sampling

This section is focused on defining the study population, discussion of the sampling method, an assessment of how data saturation was achieved, and a discussion of the setting for the semistructured interviews was observed. The population of the study was IT leaders in universities and colleges. The sample for this study was at least two top-level information technology leaders in each of at least three universities and colleges located in Southern California.

Purposeful sampling is a non-probabilistic sampling technique where research participants or investigated units are selected based on the discretion or judgment of the researcher (Gentles, Charles, Nicholas, Ploeg, & McKibbon, 2016). Purposeful sampling was utilized in the selection of study participants that satisfied all eligibility requirements to enhance data gathering to help answer the overarching question. Benoot, Hannes, and Bilsen (2016) described purposeful sampling as a viable option for an information-rich focused study. To reach data saturation, at least three qualified IT leaders in each of at least three qualified universities or colleges were interviewed.

Purposive sampling techniques were employed in the conduct of this study. Purposive sampling is a non-probabilistic technique where sample selection is based on the characteristics of the population and the objectives of the study (Onwuegbuzie & Collins, 2017). Benoot et al. (2016) explained purposeful sampling is favorable for the identification and collection of information-rich cases. Since the overarching research question sought to explore strategies that top-level universities and colleges IT leaders use to prevent malware attacks, the sampling technique must purposely target the research participants to get rich and coherent data. In this light, an expert sampling technique was adopted during the study participants' selection. Drawing from this, information technology leaders with at least five years of experience and practical knowledge of information security from universities in southern California were selected for the population. Karagiozis (2018) discussed the main objective of purposive sampling is to emphasize specific traits of the population of interest which will augment in answering the overarching research question. By using a purposive sampling technique, I was able to select study subjects with informed perspectives about the study. Therefore, the rationale for using a purposive sampling technique was to include subjects who are well versed in the area of study and ease in making a generalization.

The number of participants in a qualitative study is dependent on the number required to holistically address all facets of the phenomenon under investigation (Vasileiou, Barnett, Thorpe, & Young, 2018). According to Boddy (2016), the ideal sample size for the conduct of qualitative research ranges from five to 50 participants. Blaikie (2018) argued the relative importance of data saturation when mulling over sample size decisions in qualitative research. Sim et al. (2018) contributed to the debate, pinpointing the challenges associated with study participants' number determination. In his work, Boddy (2016) argued the determination of sample size is circumstantial and partially reliant on the scientific paradigm under which the investigation is taking place.

Data saturation is the point in the research process where data collection does not provide any new or relevant information (Blaikie, 2018). It is an instance in the research process where gathering new data fails to spark new theoretical insights nor shows new traits of the core theoretical categories. Data saturation was attained in this study when new data seems to be redundant of already collected data. Lowe, Norris, Farris, and Babbage (2018) stated that data saturation depends on factors such as heterogeneity or homogeneity of the study population, selection criteria, study budget, the existence of key stratifies, timelines, and researcher experience. Tran, Porcher, Tran, and Ravaud (2017) implied failure to reach data saturation infringes on the quality and validity of the conducted research. Tran et al. (2017) emphasized interviews as one method by which data saturation can be attained. Lowe et al. (2018) recommended structuring interview questions in a way to facilitate posing the same question to multiple participants to reach data saturation. In this study, data saturation was achieved when additional data did not lead to the discovery of no new information. Another strategy to ensure data saturation was member checking where each study subject was presented with the opportunity to verify the content of recorded interview responses. Data saturation in this research was attained through the gathering of data from multiple sources geared toward strategies IT leaders use to prevent malware attacks in colleges and universities until no new information is uncovered. Interview data, gathered institution documents, and discovered strategies in the literature review served as the main sources of triangulation in this research.

In this study, a conducive and serene environment was adopted for the conduct of the interview devoid of distractions and to augment open dialog between study subjects and researchers. O’Keeffe, Buytaert, Mijic, Brozović, and Sinha (2016) explained the importance of a serene environment for the conduct of research interviews. Study subjects were interviewed at their respective offices in the university and college of jurisdiction or based on the participants’ location choice. To establish an effective data collection exercise, I ensured the interview setting is devoid of distractions but conducive for open discussion. Brown and Danaher (2019) discussed the importance of interview location since it can affect the gathering of data and therefore must be devoid of conditions that impair participants' convenience and comfort. Drawing from this, study participants decided the most appropriate setting for the interview. Skype or Zoom meetings were provided as an option for study participants to participate in the interview as an additional layer of fostering convenience. As noted by Kallio, Pietila, Johnson, and Kangasniemi (2018), study subjects must be convenient in the disclosure of information about the research.

Ethical Research

The informed consent form is a voluntary document or agreement between the researcher and study participants to participate in a study. The informed consent form serves as a prerequisite for study subjects' participation in research. A copy of the informed consent form was attached to the study subject's invitation to participate email in addition to the reason for the conduct of the study, study questions, and my contact information for prior questions. According to Kyegombe, Banks, Kelly, Kuper, and Devries (2019), obtaining consent encompasses informing study subjects about their rights, the objective of the study, the procedures, and the possible perils and benefits of involvement. Kyegombe et al. stated that informed consent safeguards the rights of all study participants are not violated. As noted by Mootz, Taylor, Wainberg, and Khoshnood (2019), the objective of the informed consent process is to furnish study participants with sufficient information to foster a well-versed decision to enroll or be excluded from the research. Mootz et al. argued the informed consent form must be written in a comprehensible language, lacks the undue influence to study subjects, and provides adequate time for study subjects to review material. The composition of the consent form addresses the purpose of the study, criteria for study participation, data protection, disclosure incentives, the timeframe of the study, and publication of study findings.

Potential participants were advised that research participation is entirely voluntary and that they reserve the right to be excluded from the research at any time without any repercussion as enshrined in the informed consent document. According to Ellis (2019), researchers must consider participants’ mental, physical, and emotional abilities while seeking human subjects’ consent before proceeding with the research. To avoid study bias, no incentives were provided to the study participants with a notice to that effect. Okyere (2018) explained the provision of incentives in the conduct of research fosters biased study findings. Study subjects will not be given any form of incentives to induce participation.

All the legal and ethical considerations as stipulated by the Walden University IRB was adhered to in the conduct of this study to safeguard the security of the study participants. In this light, the anonymity of study participants was maintained. Study subjects were given a pseudonym (e.g., P1, P2) to foster identity protection and confidentiality of collected data. As noted by Surmiak (2018), the annotation of generic code to each participant augments confidentiality and anonymity.

There is a need for researchers to maintain contact with respondent’s during and after the conduct of a study while presenting detailed accounts of subjects (Lancaster

(2017). In this light, to safeguard the confidentiality of collected data and comply with the outlined requirements of Walden University IRB requirements, all collected data were kept in a safe, and all electronic data were saved in a special folder in the cloud. Walden University's Institutional Review Board has issued the approval number 04-10-20-0736295 for this project. The repository folder was secured with a password. After five years of the date of publication, data was permanently destroyed. In this light, hard copies of research data were shredded while digital versions were permanently deleted.

Data Collection

Data Collection Instrument

I was the principal data collection instrument in this study following the role of the researcher component of the research. In qualitative research, the researcher remains the primary data collection instrument (Richard & Bélanger, 2018). Moser and Korstjens (2018) explained the researcher plays a pivotal role in terms of observing, documenting, communicating with study subjects, and the conduct of interviews. As noted by Alase, A. (2017), the researcher remains instrumental in the observation, documentation of data, conversation with study subjects during the conduct of qualitative studies. More, the researcher's attention to detail, probing for further explanation, and subjectivity during the data-gathering exercise remains intrinsic to the research process. In this light, I ensured all the necessary data needed to answer the overarching question are collected.

Secondary data collection techniques encompassed the literature review as well as relevant documents from the organizations of the participants. As emphasized by Renbarger, Sulak, and Kaul (2019), secondary data sources are beneficial since it saves the researcher time and cost associated with gathering new additional data to enrich the study exercise. In the same vein, Prada-Ramallal, Roque, Herdeiro, Takkouche, and Figueiras (2018) claimed secondary data have the attribute of a pre-established validity. Secondary data plays an intrinsic role in the concept of data enrichment (Andrei, 2018). Drawing from this, before the utilization of secondary data, reliability, suitability, and adequacy of collected data was ascertained. The research topic, the purpose of the study, and the conceptual framework served as a guide in the collection of the necessary data to help answer the overarching question.

I employed a semistructured interview in the gathering of raw data from study subjects following the interview protocol. According to Brown and Danaher (2019), a semistructured interview augments the gathering of intensive qualitative data by asking open-ended questions. A semistructured interview is popular for resorting to a dialogue between the researcher and the participants and therefore is more appropriate for gathering rich data qualitative research (Vila-Henninger, 2019). Brown and Danaher contended the open-ended nature of semistructured interview questions fosters a detailed discussion of topics under investigation leading to the gathering of rich data. Drawing from this, semistructured interview associated benefit of in-depth data gathering coupled with higher chances of follow-up questions with the collected data play a key in selecting a semistructured interview instrument.

Interviews, focus group discussions, observational methods, and document analysis are some of the notable examples of data-gathering instruments (Carr, Zhang, Ming, Hung, & Siddiqui, 2019). As noted by Carr et al. (2019), interviews are beneficial in exploring subjects' experiences, opinions, views, and beliefs concerning the topic under investigation. Carr et al. explained observational methods used to gain insight into a phenomenon by observing users' accounts in an everyday context. A semistructured interview is a data-gathering instrument where the interview process is open, paving way for the development of new ideas during the interview due to the response of the interviewee. The interviewer in a semistructured interview mostly is guided by a framework of themes to be explored. A semistructured interview technique involves a formal conversation between the interviewer and respondents. In this light, I utilized a semistructured interview to gather a comprehensive set of data in this study to help answer the overarching question.

An interview protocol (Appendix C) was utilized in the conduct of this data collection exercise. Using the interview protocol, I provided an overview of the interview process (see details in Appendix C). Interview confidentiality was communicated to participants after they have agreed to be recorded. Interview recordings were in after announcing study subjects' alphanumeric code, date, and time. Interview sessions lasted approximately 30 to 60 minutes and were communicated to study participants. The concluding section of the interview was focused on an explanation of the concept and overall plan. Responses to questions were confirmed with study subjects for clarification and satisfaction purposes and proceed to end the interview with an appreciation note for honoring the invitation. Deploying the interview protocol will help to address all research questions as reflected in an orderly fashion and is depicted in Appendix C. In the same vein, I followed topical trajectories during the conversation that may deviate from the already agreed guideline if deemed appropriate.

To ensure the reliability and validity of the collected data, I used respondent validation also known as member checking. Birt, Scott, Cavers, Campbell, and Walter (2016), in their work, explained member checking fosters the gathering of accurate, credible, and valid information in a qualitative research setting. In this light, every study participant was provided with an opportunity to verify if the gathered information reflects their views, experiences, and emotions as described. For study participants to volunteer further information that may be stimulated by the playback process (Birt et al., 2016). DeCino and Waalkes (2019) stated member checking provides the opportunity for the study subjects to rectify any errors in the collected data and to challenge erroneous interpretation. Drawing from the works of DeCino and Waalkes, I adopted member-checking to enhance the reliability and validity of the data collection instrument. Member checking was achieved by providing the summarized bullets of the interview results to study participants to verify for accuracy. Drawing on this, I scheduled a second interview with study participants either face-to-face or by phone depending on the participant's choice to go over the transcribed version of the interview.

Data Collection Technique

In this study, I employed a semistructured interview in the data gathering process of this study. Since my research involved an exploration of strategies IT leaders in universities and colleges use to prevent malware attacks, I chose an interview technique as the most appropriate data collection technique. Clark and Vealé (2018) argued semistructured interview is more applicable to instances where the researcher intends to gather in-depth qualitative textual data. Shapka, Domene, Khan, and Yang (2016) in their work posit the interview technique facilitates a balance between the versatility of an open-ended interview and the emphasis of a standardized ethnographic survey. The interview data collection technique is more utilized during the beginning and later stages of exploratory research (Cataldi, 2018). According to Anselmi, Fabbris, Martini, and Robusto (2018), an interview data collection technique can reveal rich descriptive data on the personal experience of the study subjects. Information collected through a semistructured interview can serve the purpose of addressing general domains of the research topic as well as more specific insights (Anselmi et al., 2018).

A semistructured interview was used as a data collection technique for this research. The interview started with an overview of the research topic after research participants had consented to be part of the study. I proceeded to show my appreciation to each research participant for honoring the invitation to participate in the research. Research participants were then informed the interview will be recorded and proceeded after they have consented to be recorded. After research participants granted permission to proceed with the recording and I asked the necessary questions about the research. The duration of each interview lasted around 30 to 60 minutes until all questions were answered. Study subjects were asked to provide any organizational documents in support of the interview responses. A second interview, either face-to-face or by phone depending on the participant’s choice, was dedicated to member checking. In this case, member-checking was observed by furnishing study participants with the transcribed version of the interview for accuracy and validity in a short follow-up interview. The interview ended with a thank you to research participants once all question responses had been confirmed to the satisfaction of the study participants.

Interview data collection technique is advantageous because it fosters the gathering of detailed information about the research by plunging deeper into the study subjects' responses, feelings, and opinions (Shawver et al., 2016). Gauchi (2017) emphasized the adoption of Skype video calls are less expensive relative to face-to-face and enhances access to any study subject irrespective of their location. Telephone interviews can augment a measure of anonymity during the data collection exercise (Gauchi, 2017). Interviews augment detailed questions to be asked plus facilitate the achievement of a high response rate. Interviews augment the resolution of ambiguity and the clarification of incomplete answers through member-checking which contributes to the validity of collected data (Brown & Danaher, 2019). Conversely, interviews can be time-consuming especially during the process of setting up, conducting the interview, transcription, analysis of collected data, feedback, and reporting (Brown & Danaher, 2019). More, different study subjects may interpret interview questions differently leading to varied responses (Brown & Danaher, 2019). The interview questions can be found in Appendix D.

Drawing from this, member checking was utilized in this study to improve the correctness, trustworthiness, and validity of gathered information. Member checking was also used as an avenue for study subjects to volunteer for more information about the chosen topic. The interviews were recorded, transcribed, and summarized into very few bullet points after transcription. The bulleted summary was discussed in a short 10 minutes interview with the participants with a request for the interviewee to verify the accuracy of their summarized statements.

Data Organization Techniques

Because of the large amount of collected data in qualitative case study research, there remain certain types of techniques that can be adopted in data organization and management. According to Alase (2017), a researcher should consider the utilization of research notes, interview transcriptions, and research logs to warrant the reliability and validity of a study as well as the discovery of themes and patterns. In this light, I maintained a research log throughout the conduct of this study to augment the data organization and to contribute to the validity and reliability of the study. As stated by Osborne (2016), the research log is beneficial to the researcher in terms of sorting out what has and has not been discovered as well as to capture data and themes. Drawing from this, the research log was utilized to track study notes, interview observations, and to discover possible research themes. Pangeni (2017) contended that the research log can be used in the organization and correlation of gathered information from the research. More, Pangeni (2017) stressed the importance of the research log noting its ability to save an enormous amount of time by avoiding repetitive searches after a study exercise pause. In contribution to the value of the research log, Clark, Birkhead, Fernandez, and Egger (2017) claimed the exercise helps the researcher to weigh evidence to foster drawing better conclusions and lineage connections. Throughout the conduct of this study, the research log was beneficial in the arrangement of thoughts and correlated ideas coupled with presenting an enabling environment for me to arrange themes and avoid data redundancy.

Collected data was transcribed using Microsoft Word and NVivo applications. To protect the identity of the study subjects, each participant was uniquely assigned an alphanumeric code such as P1, P2 for participant 1, and participant 2 respectively. All electronic data will be stored in a password encrypted cloud folder for five years from the publication date. Hard copies of collected data will be securely stored in a locked file cabinet in my home in addition to any other related documents of the research. After five years, all hard and digital documentation of research data will be permanently destroyed. In this light, I will shred all hard copy documentation of the research while digital copies will be permanently deleted from both the cloud and hard drives.

Data Analysis Technique

Thematic data analysis was the chosen data analysis technique for this study. Castleberry and Nolen (2018) stated thematic analysis encompasses an identification, analysis, and interpretation of patterns of meaning inherent in qualitative data. Thematic analysis is an umbrella term used to address a set of approaches for analyzing qualitative data focused on identifying themes. According to Sahin (2018), methodological triangulation augments the gathering of more comprehensive data that contributes to research topic validity by fostering an element of cross-checking. I utilized methodological triangulation to validate the findings of this multiple case study. IT leaders in universities and colleges through a semistructured interview served as a data source coupled with organizational documentation. Abdalla, Oliveira, Azevedo, and Gonzalez (2018) argued the adoption of multiple sources of data contributes to the accuracy of triangulation. Nvivo v. application was used in the processing and organization of the gathered information associated with the study. Methodological triangulation augments the validation of study findings (Ogarkova, Soriano, & Gladkova, 2016). Drawing on this, the overall validity of the study coupled with the discovery of patterns in the data analysis stage was achieved by using methodological triangulation of the transcribed data in addition to already gathered institutional documents. Interview data and institutional documents will serve as the main sources of triangulation in this study.

The main objective of the data analysis stage of this study was to discover themes from the raw gathered data. Scharp and Sanders (2019) in their work posited thematic analysis denotes an iterative procedure of gathering nonstructured data and proceeding to map out the most important themes. Scharp and Sanders enumerated six steps for conducting a thematic analysis—data familiarization, assignment of preliminary codes to data to foster content, exploration of patterns or themes with codes across the various interviews, theme revision, theme naming, and definition, and report production.

Familiarization with collected data was the first phase of the thematic analysis process. All audio recordings were transcribed in addition to going through all the entire interview data coupled with taking notes. I marked down preliminary ideas that address the intended content of the study at phase one of the thematic analysis. Considering the dictate of phase one of the thematic analysis, I reviewed interview transcripts from each study participant in addition to any member checking information to ascertain a detailed understanding of the data. Additionally, I systematically reviewed the provided institutional documentation about the established policies and procedures for preventing malware attacks. Research notes were gathered in the process of reviewing these documents and contributed to the generation of initial codes. The comprehension and interpretation of these codes added to the initial development of inherent codes and key research themes. The proceeding phase of the thematic analysis was built on the general knowledge of interview and organizational data.

Phase two of the thematic analysis entailed the generation of initial codes. A code addresses a brief description of what is said in an interview. Coding is a term used to describe the process of detecting passages in a text, probing and detecting concepts, and finding relations and patterns between them (Mackieson, Shlonsky, & Connolly, 2019). Code implies a description and not an interpretation and is an approach to start organizing interview data into meaningful categories. The coding was based on phrases and words related to malware attacks. NVivo software was utilized to uncover themes and patterns in the gathered data. NVivo computer software is a qualitative data analysis tool designed to work with rich text-based or multimedia data where a detailed level of analysis on small or large volumes of data are needed. The NVivo software tool was used to discover recurring themes in the gathered interview data coupled with creating an association with interview responses. Rothgangel and Saup (2017) described axial coding as the breakdown and identification of relationships among the central themes in qualitative research data analysis. In this light, axial coding was used at this phase of the data analysis to create links, categories, and associations among groupings, establish significant and minor themes.

In phase three I wrote codes on sticky notes to augment easy move around, visualization purposes, and to help capture the relationship between the different codes and the level of the themes. Phase three is focused on the identification of themes by observing the list of codes plus their associated excerpts (Castleberry & Nolen, 2018). After extraction, codes should be collated to broader themes that present information about the collected raw data (Roberts, Dowell, & Nie, 2019). The practice of searching for themes is an iterative procedure that requires the movement of codes to form different themes concerning the study (Mackieson et al., 2019). In the words of Roberts et al. (2019), during the theme selection process, the researcher should focus on frequently used words by the study subjects, streamline the themes, create a hierarchy of themes, and connect the discovered themes with the conceptual framework and the research question. I borrowed from the strategy outlined by Roberts et al. (2019) at this phase of the thematic analysis.

Phase four of the thematic analysis emphasized on a review and refinement of the identified themes in phase three. I reviewed all extracted codes to ascertain if they support the discovered themes, contradict, or overlap. As stated by Belotto (2018) there should be meaningful coherence between the data within themes in addition to clearer and perceptible distinctions between them. The existence of contradictions within themes or broader themes is enough reasons to separate or move such themes into an existing one where they might fit better (Lehmann, Murakami, & Klempe, 2019). Drawing from the words of Lehmann et al. (2019), during the process of theme and code review, all broad codes or themes that contradict others were split or added to the ones where they harmoniously fit.

Phase five of the data analysis exercise was dedicated to defining and naming themes. At this stage of the thematic analysis, names and descriptions were assigned to themes identified in the previous phase. As emphasized by Scharp and Sanders (2019) assignment of theme names should be descriptive and engaging. In this light, I explained what the theme entails coupled with a documentation of the essence of the theme and why it relates to other themes and the overarching research question. At this phase of the analysis, central themes were uncovered and defined by observing the frequency of occurrence and making a comparison with the literature review and the conceptual framework.

The last phase of the thematic analysis focused on the generation of a report about the major and minor themes coupled with how each theme ties into the literature review and the conceptual framework. At this stage of the thematic analysis, the inbuilt capabilities of NVivo software were utilized in creating such a connection. The inherent capability of creating word clouds, treemaps, and cluster analysis of NVivo software was significant in the report generation.

Reliability and Validity

Dependability

Dependability in qualitative research addresses the stability of data over time and conditions (FitzPatrick, 2019). Smith and Smith (2018) described reliability as an assessment of the quality of the data collection and analysis processes. Drawing on this, I provided a succinct set of notes on decisions made during the research process, utilized research materials, sampling, and the emergence of findings related to data management. In the words of Moon, Brewer, Januchowski-Hartley, Adams, and Blackman (2016), qualitative researchers understand the fact that reality remains a social construct and continuously evolves. More, Moon et al. (2016) posited dependability emanates from capturing the evolving conditions associated with the setting and the study design because reality is socially constructed. Jordan (2018) claimed a dependable study must exhibit accuracy and consistency. Collingridge and Gantt (2019) also, postulated reliability and validity are identical to credibility and dependability.

Member checking and triangulation methods were utilized to achieve dependability in this research. Member checking plays a significant role in ensuring research dependability (Birt et al., 2016). In this light, member-checking was utilized by furnishing each study subject with a transcribed version of gathered interview data for accuracy and consistency. According to Holt and McHugh (2018), member checking augments study participants the opportunity to clarify, rectify, and provide additional information on interview data. As stated by Birt et al., data misinterpretation impairs the validity and creditability of the study. Member checking was utilized in this study during the follow-up process to verify the interpretation of gathered interview data reflects the intended responses of study participants.

Credibility

The credibility of qualitative research involves the establishment of the tenet of trustworthiness and integrity of the study findings. Amankwaa (2016) said member checking simultaneously contributes to research credibility and enhances the relationship between study participants and the researcher. Member checking plays a significant role in increasing the trustworthiness and reliability of a study (Liao & Hitchcock, 2018). I used the tenets of member checking to enhance the credibility of this study by allowing study subjects to rectify any erroneous interpretation gathered during the interview process. According to Anderson (2017), in addition to assessing the accuracy of collected data, member checking also fosters the development of a cordial relationship between study subjects and the researcher contributing to research credibility. Member checking was utilized to ensure the accuracy of collected data and also reflects the real intent of research participants.

Methodological triangulation was used to complement the validity and credibility of this study. Abdalla et al. (2018) described triangulation as a strategy to enhance research validity and reliability through the convergence of data from varied sources. According to Fusch et al. (2018), researchers should consider the adoption of triangulation to foresee validity and reliability in study findings. In this study, triangulation was achieved through the conducted interviews, institutional documents about the topic, and other related operational documents.

Transferability

Transferability is the extent to which the findings of a qualitative study can be generalized or transferred to other contexts or situations (Ferrando, Hoogerwerf, & Kadyrbaeva, 2019). As stated by Carminati (2018), transferability pertains to the ability to apply the results of a study to multiple settings or broader groups. To augment the applicability of my research to various settings, I provided a robust description of my experiences during the data collection process and other related practices. It is the sole prerogative responsibility of the researcher to present the information that augments possible transferability judgment but not the deterministic factor (Forero et al., 2018). To contribute to the transferability of this study, I presented a thorough description of the context and the assumptions central to the conduct of the research. As emphasized by Weil (2017) researchers should give a detailed account of events surrounding the study; researchers should assess the extent to which conclusions can be applied to other situations, people, and settings.

To contribute to transferability, Hartblay (2018) recommended the adoption of the full description. Hartblay described the full report as a procedure for achieving external validity through a detailed portrayal of events or experiences during data collection. Transferability was achieved in this study through the utilization of all the prearranged protocol for conducting qualitative research, which in this context pertains to the presentation of enough information data readers can utilize to determine the study's transferability.

Confirmability

Confirmability is the provision of evidence that the research study findings reflect participants' narratives and words but not possible researcher bias (Korstjens & Moser, 2017). Confirmability is an inherent component of the survey that verifies if results are shaped by study subjects' views rather than researchers' (Connelly, 2016). To attain research confirmability, Hadi and Closs (2016) recommended researchers give a detailed description of the processes leading to data collection, analysis, and interpretation. To achieve confirmability and trustworthiness in this study, I used a detailed description of the methodologies relating to the conduct of the study coupled with seeking study subjects’ views in terms of validity and conclusion. Also, every study subject was given the transcribed version of the interview during a short follow-up interview to assess for accuracy and legality.

Data Saturation

Data saturation signifies the stage in the research process where no new information or themes are discovered during data analysis and signals the need to cease data collection (Tran et al., 2017). In this study, triangulation was achieved by two sources of information: interview results and company documents. Member checking was achieved by providing the summarized bullets of the interview results to study participants to verify for accuracy. Data saturation was attained by interviewing a second person within a university then comparing the results of the first two interviewees to ascertain if they have disclosed similar information. If not, then a third person was interviewed, and others were added until no new information is revealed. This exercise was replicated for the next university, interviewing at least two participants and comparing the results. The same exercise was replicated in a third university comparing the interview results to ascertain the similarities or discrepancies. After saturation was verified within each university, interview responses were compared across all three universities. If there were similarities among information gathered from all three universities, then saturation is achieved, and data collection will end. If some information came from only one university, then a fourth university was added until themes and responses reflect similarities. As stated by Thomas (2017), member checking augments the reduction of a conflicting and erroneous interpretation of interview data before data analysis. Varpio, Ajjawi, Monrouxe, O'Brien, and Rees (2017) claimed that member checking enhances research data saturation, research validity, and reliability. In this light, study participants were contacted for a second interview, either through phone or face-to-face based on participant's choice, to review the collected interview data for clarity and accuracy as stipulated in the interview protocol. According to Lowe, Norris, Farris, and Babbage (2017), data saturation is achieved when there is redundancy in collected data, and failure to reach this stage impairs the study findings quality. Data saturation is a step in the study process where the researcher is assured probing further to gather additional information will yield similar results and repetitive information and themes leading to data redundancy (Tran, Porcher, Falissard, & Ravaud, 2016). Saunders et al. (2018) recommended researchers explain how, when, and to what extent data saturation is achieved.

Transition and Summary

Section 2 of this study was focused on the main purpose of the study, the target study participants, strategies, and methods for data collection, analysis, and organization, population and sampling have been addressed. The objective of this qualitative multiple case study was to explore strategies of information technology leaders in universities and colleges use to prevent and mitigate malware attacks. Methodological triangulation was employed to establish the validity and credibility of this qualitative multiple case study. In Section 3, this study was focused on the presentation of findings, application to professional practice, implications for social change, recommendations for action and further study, reflections, and a strong concluding statement.

Section 3: Applications for Professional Practice and Implications for Social Change

Introduction

The purpose of this study was to explore strategies that colleges' and universities' IT leaders use to prevent and mitigate malware attacks to information systems.

Four major themes were uncovered during the thematic analysis phase of the study. Evidence from the interview data confirms the use of programs that address personnel issues, the first major theme, as one of the most significant strategies for dealing with malware threats that result from user behavior. Security planning was the second significant theme to emerge during the thematic analysis phase of the study. Security planning involves the set of guidelines and procedures for all individuals gaining access to and using the institution's systems and resources. Moreover, security planning guides specific activities and practices concerning the performance of information security tasks and functions. The third theme of security management practices is focused on the implementation of existing tools to achieve maximum system security. Security management practices deal with assessment of an institution's information assets and devising of policies, measures, guidelines, and procedures to establish information assurance. Ethical hacking was the last theme to emerge during the thematic analysis phase of the study. Ethical hacking deals with the proactive and reactive strategy of probing existing systems for vulnerabilities and coming up with resolutions. In this light, some study participants expressed the need for early vulnerability detection and application of required patches before vulnerabilities can be capitalized upon by malware.

In the subsequent sections, I present applications to professional practice, implications for social change, recommendations for action, recommendations for further research, and reflections.

Presentation of the Findings

The overarching research question that drove the conduct of this research was the following: What strategies do universities' and colleges' information technology leaders use to prevent malware attacks to information systems?

To help answer the overarching question, I used semistructured interviews to collect data from all study participants. Three higher education institutions in Southern California participated in the research. Three study participants from each of the three partner organizations agreed to provide information to help answer the research question. All nine participants were given a pseudonym (e.g., P1 for Participant 1, P2 for Participant 2, etc.) to help establish confidentiality and to prevent the disclosure of personal identities.

This section is focused on a critical analysis of the four major themes discovered during the data analysis phase of the study. I utilized methodological triangulation to analyze both the interview data and institutional documents related to malware attack prevention within universities and colleges. Member checking, interview transcripts, and institutional documents were uploaded into NVivo 12 software to enable analysis of the data. The NVivo software data analysis produced four major themes: (a) malware training and awareness, (b) information security policies and procedures, (c) security management tools and techniques, and (d) ethical hacking. According to Le Blanc

(2017), NVivo applications augment visual analysis and coding of gathered data into themes. The thematic analysis phase was tied into the literature review and the conceptual framework of the study after themes were discovered.

In the following subsections, I discuss each theme coupled with the expressed views of the study participants concerning it. Additionally, I address each of the four major themes unveiled during the thematic analysis phase in relation to other scholarly studies, GST as the conceptual framework of this study, and effective IT practices.

Theme 1: Personnel Issues

Overview. Personnel issues were the first significant theme to emerge during the data analysis stage of the research. Leaders of higher education institutions, as well as other corporate organizations, consider their information systems to be exposed to security threats largely because of unscrutinized user behaviors and activities (Wijaya, Gunawan, Avrizal, & Arif, 2020). The leaders of most higher education institutions use malware training and awareness programs to inform employees and stakeholders about potential threats, thereby protecting their systems. Table 1 depicts numbers of references related to the personnel issues theme and its subthemes.

Table 1

References to Personnel Issues

Major theme	Participants		Documents	
	Count	References	Count	References
Personnel issues	9	83	7	7
Subthemes:				
Security training	5	44	4	4
Security awareness	4	39	3	3

Findings from participant interviews and organizational documents.

Security training**.** Training was one of the significant subthemes to emerge during thematic analysis. According to all study participants, training was employed by partner organizations to address personnel issues. As stated by P9, “user training is imperative to address all the human vulnerability in the network or system and their perspective about data security threats.” In the same vein, P1 noted that “the IT department trains users to watch out for social engineering emails, bad software, and any other threats to take advantage of the system.” P3 presented a similar view about user training, saying, “we also had internal training to help employees to know what to do if something big like malware that threatens the confidentiality of data or systems happens or even something little.” Evidence from the study shows that malware training may help improve employee perspectives about security and responses to information confidentiality threats. In alignment, P5 claimed, “simulated attacks training has been very effective in influencing system user perspective about the malware and other security threats.”

Seven out of the nine study participants emphasized the adoption of annual training to educate employees and other system users about the existing threats that their institution faces. In that vein, P4 advocated “better training which is annually scheduled in the academic year.” P5 shared a similar view about the number of times that the institutions’ security training is scheduled: “In addition to the automatic training linked to the simulated attacks, we do have annual information security training to employees.” P6 further noted, “we’ve done training every 4 to 5 months with certain staff which is organized every year within the school.” P7 contributed to the same timeline for conducting training for the system userbase to bring to light new methods of malware attacks. In the words of P7, “In this environment, we do get annual refresher training, security, refresher training.”

The participants defined automatic training as pieces of teaching moments or sessions triggered when system users click on simulated attacks within the network. Some study participants described the adoption of automatic training associated with routine simulated attacks to test the effectiveness and retention of security training. As stated by P3, “employees are directed automatic training when they click on false suspicious links to test their alertness to system threats.” P4 shared a similar perspective on the effectiveness of automatic training: “The automatic training is leading to people being more aware and informs their views about the threats.” To emphasize the effectiveness of malware training, P6 claimed, “So we use that as a tool to train people who click on those simulated links and it has been very effective.”

Although five out of the nine study participants expressed the positive impact of malware training on data security, two out of the nine expressed some challenges with the strategy. P4 remarked, “you know, one of the problems with training is that you know, measuring the effectiveness of it, that that's still a work in progress.” To address this challenge, P4 claimed that the institution had adopted automatic training associated with simulated attacks. P4 characterized these as “simulated attacks, but that's all they are, simulated techniques, simulated phishing. And when we do those, we can get metrics and metrics have been positive.” On the other hand, P2 expressed, “So I have one staff member that gets the training in malware. I have had a difficult time retaining them long enough to both train them and get the value out of that training." Two out of the nine participants expressed some concerns with the implementation of malware training due to a lack of metrics to measure its effectiveness in the real world, as well as low employee retention. P4 claimed a lower percentage of trainees who apply information acquired through the training. However, six out of nine study participants supported the significant role that training plays in educating users about malware mitigation and prevention strategies and threats to confidentiality for the institution as a whole. As stated by P4, "So, yes, we did do a combination of cybersecurity awareness training for end-users and it has been very effective in creating security mindfulness in the IT department and the school."

Security awareness. The findings of the study support the contribution of malware awareness programs in creating a culture of security consciousness. Seven out of nine study participants supported the effectiveness of security awareness programs in creating security mindfulness in their respective working environments. As confirmation, P4 noted, "So, yes, we did do a combination of cybersecurity awareness training for end-users and it has been very effective in creating security mindfulness in the IT department and the school." P6 explained, "we do a lot of training and awareness programs with the staff and faculty at the campus in the year, I think those awareness programs are working to direct a security atmosphere which we love."According to P5, "malware awareness programs ensure that system users and stakeholders are sensitized and are fully cognizant about the repercussions of failing to comply with policies to protect the institution's system and network from both internal and external threats." As stated by P1, “employees that fail to adhere and comply with the security awareness training are subjected to consequences leading to possible termination.” In the same vein, P3 expressed, “It is a policy in conjunction with the human resource department for security awareness program compliance to help create a security culture.” In a similar view, P5 confessed, “So you see, our security awareness programs are ingrained in our policy which employees are supposed to read and adhere to. With that, it helps with absolute acceptance and use.” A similar perspective was held by P7: “we employ some of the best state of the art intrusion detection systems and we also enforce annual security awareness and training.”

Four of the interviewed participants had adopted an institutional policy focused on requesting employees’ and end users’ compliance with awareness programs. P1 explained, “Our annual security awareness and training are mandatory for all employees and contractors. Employees that fail to adhere and comply with the security awareness training may be penalized according to the tenets of the institution.” Likewise, P3 noted, “So we request annual employee training. Our training is structured in a way that is central in ensuring all users comply with practices against malware attacks.” P9 acknowledged that it

> is challenging sometimes dealing with humans especially when it comes to censoring their activities. But implementing policies that are binding on all system users to follow through with the universities’ security training and requirements has been very productive and helpful to our network.

Seven out of the nine study participants claimed that their security awareness program had been supported by a policy requiring adherence and compliance to foster the program's successful implementation and adoption. To emphasize the indispensable security awareness programs within the institution, P9 stated, "if an organization does not have an effective security awareness and training program, then all technology solutions will fail."

Based on the collected and analyzed data from the study, three participants emphasized the significant role that security awareness programs play in modifying the security culture within the institution, suggesting that without awareness efforts, the security program would fail. For example, P3 stated,

> our training is structured in a way that is central in ensuring all users comply with practices against malware attacks. It is a policy in conjunction with the human resource department for security awareness program compliance to help create a security culture.

Gathered evidence on the perspectives of the study participants shows that security training and awareness contribute to sensitizing employees across the organization about data confidentiality threats, hence helping to deal with personnel issues. As recapped by P5, "overall some administrators and employees have confessed how the pieces of training have broadened their perspective about malware and information security."

Company documentation support for personnel issue. The significance of this theme was emphasized by four organizational documents used for methodological triangulation. Evidence from Partner Organization A Document 1 denoted the need for all

IT personnel and employees to follow and abide by the guidelines concerning security training and awareness. Document 2 from Partner Organization A further confirmed the need for stakeholders and system users to participate, comply with, and utilize the tenets of security and awareness training to secure systems and sensitive data. Additional documents from other partner organizations stipulated consequences for noncompliance with security and awareness programs. For example, Document 3 from Partner Organization B specified repercussions for failing to participate and enroll in security and awareness programs. In the same vein, Partner Organization C emphatically stated the need for employees or system users to automatically enroll in a mandatory 20-minute security training due to unwarranted activities that subject confidential data to threats. Document 4 from Partner Organization D reiterated the use of KnowBe4 to direct automatic security training and awareness to all employees who accidentally fall victim to simulated attacks. Considering the adoption of these policies and documentation, employees and stakeholders were educated with appropriate strategies to address situations that threaten the confidentiality of institutional digital assets.

Four out of the seven observed documents contained requests for employees and stakeholders to enroll in mandatory annual training to help steer users away from activities that might subject confidential information and systems to security risks. For example, Document 1 from Partner Organization A stipulated mandatory security training for users who demonstrate careless technical behaviors. Document 2 from Partner Organization B articulated the need for employee annual security training to address diverging conceptions about information security threats. Documents 3 and 4 from Partner Organizations C and D, respectively, followed a similar pattern of advocating annual training and awareness for all stakeholders to support the fight against data breaches. Three out of the nine participants claimed that employees and stakeholders are required to read and adhere to all information security policies about malware training at the university or college.

Connections to effective information technology practice. Seven out of nine study participants emphasized the indispensable role that malware training and awareness play in informing stakeholders about the risks and threats inherent in their network. Additionally, five out of the seven organizational documents supported this assertion. In alignment, Maiorca, Demontis, Biggio, Roli, and Giacinto (2020) stressed that end users should rectify suspicious and unsafe practices through effective malware training and awareness whereby they are educated to avoid being vectors of software attacks. Lim, Park, and Lee (2016), in the same vein, emphasized the need for employee training and awareness to be combined with security processes to help deal with data threats caused by social engineering, careless activities, suspicious emails, and links.

Ding, Wu, and Zhang (2019) claimed that most cybercriminals capitalize on human weakness to perpetuate the deployment of bad software into organizations' networks and that the adoption of robust user security training must therefore be encouraged. All nine study participants echoed the assertion of Ding et al. (2019) emphasizing the need for effective security training to expose end users to new and advanced strategies for dealing with malware attacks. As stated by Choi et al. (2018), to measure the effectiveness of security training and awareness programs, training effectiveness must be assessed using surveys in conjunction with user logs and other network metrics.

In addition to stressing the critical role information security training and awareness play in teaching users about malware threats, four out of nine participants emphasized the need for IT leaders to utilize feedback mechanisms to assess the effectiveness of the strategy as an additional layer to foresee effectiveness. Reid and Niekerk (2016) in their work about decoding audience interpretation of security awareness campaigns message, stressed using active audience and other feedback mechanisms in detecting deviations between campaign messages and the target audience perceptions and applicability. The idea of using surveys to gather feedback to measure the effectiveness of malware or data breach training and awareness programs align with Reid and Niekerk (2016) who emphasized the utilization of the strategy to decode misinterpretation associated with security campaigns. Also, four out of seven institutional documents support the need for an effective feedback process to track or measure the impact of training and awareness programs on their security landscape. Hagen, Albrechtsen, and Hovden (2008) in a documentation of the effectiveness of organizational information security measures present an assessment of existing security and awareness programs taking into consideration policies and procedures.

Moreover, evidence from the presented views of five study participants shows how automatic malware training and awareness programs help reveal risks to the institution's network and confidential information. As explained by Kim, Homan, and Metzer (2016), a precursor to individual information security behavioral changes is increasing knowledge about security threats: persistent employee information security knowledge exposure leads to changes in perspectives about malware threats and risks within the organization. In as much as study participants expressed the indispensable role security and awareness training play in sensitizing stakeholders about threats to confidential data, three out of nine participants disclosed some challenges with the strategy. Drawing on the presented challenges with security training and awareness, information retention, application, and the existence of limited metrics to assess its effectiveness were common challenges with malware training and awareness programs. As noted by Jaf et al. (2018), irrespective of the number and level training employees or system users enrolled in, there will always be some percentage that fails to apply acquired knowledge because of information retention challenges. The content of six organizational documents portrayed the need for the respective IT department to consistently schedule security training programs that inform users about recent strategies to deal with network and system threats.

Gathered data from the perspective of all nine participants further elaborates on the pivotal role malware training and awareness play in changing the perspective of system users about bad software and its threat to confidential data. As stated by Hina, and Dominic (2020), security awareness programs cannot be ruled out in the quest to achieve confidentiality, integrity, and availability of organizations' data assets and security culture. All nine study subjects' view aligns with that of Hina, and Dominic's (2020) which entrenches the indispensable role security training and awareness play in educating employees about the importance of data security, the utilization of security tactics, reportage of security violations as well as their responsibilities as engrained in the organization security policies.

According to Venter, Blignaut, Renaud, and Venter (2019), human factors and technological tools determine the success or failure of malware attacks therefore training and awareness programs should not be underestimated. In alignment, evidence from the study denotes the human element a significant piece and but most vulnerable in a security system, therefore effective training and awareness campaigns need to be revamped to address user errors and activities. As stated by Venter et al., the most security-savvy individuals are still vulnerable to unknown system vulnerabilities, and even the most robust security mechanisms can be evaded because of irresponsible user behaviors. In a similar perspective, Aldawood, and Skinner (2019) pinpointed the need for organizations and institutions to adopt processes and programs focused on educating its employees about strategies to detect and combat malware attacks. Indications from the study show the implementation of programs and campaigns geared towards educating employees and other stakeholders about the best approaches to deal with data breach threats.

Five out of the nine study participants, claimed most security gaps are a result of a lack of information security training and awareness within higher education institutions. According to Adu and Adjei (2018), coaching and training remain two of the most effective strategies for preventing and mitigating malware attacks caused by user errors within most institutions. The perspectives of the interviewed participants in the study align with Adu and Adjei's (2018) recognition of coaching and training as one of the most effective strategies for preventing and mitigating malware attacks. Also, drawing on the perspectives of the study participants, one of the strategies to address the security gaps and non-compliance challenges, three participants claimed systems users and other employees are required to read and adhere to the tenets of policies about malware training and awareness. Jaeger, Eckhardt, and Kroenung (2020) in their work posits the effectiveness of multilevel sanctions in changing information security awareness and policy compliance within an organization.

Evidence from the literature supports the theme of personnel issues as a key strategy in preventing malware attacks in universities’ and colleges’ information systems. According to Valiente (2017), educating system users and stakeholders about practices that threaten the credibility of confidential data also contribute to knowledge about information security strategies. Seven out of nine study participants emphasized the need for higher education institutions to consider security training as pivotal in ensuring that all employees and stakeholders are exposed to the principles of safeguarding information systems from malware attacks.

Most malware training and awareness programs are focused on the delivery of content and process as opposed to teaching how system users can make decisions relating to systems or data security threats (Koohang, Anderson, Nord, & Paliszkiewicz, 2020). According to Chmura (2017), information security awareness and training positively impacts employees’ perspective reformation about malware threats. The findings of malware training and awareness align with the literature by demonstrating that through information security training, IT leaders in higher education institutions can have some form of influence on employees’ perceptions of malware threats. The information security leaders’ main objectives are the identification of the risks surrounding the most confidential data within the institution and devising protective strategies and measures focused on the creation of a security atmosphere through awareness and training (Haqaf & Koyuncu, 2018).

Existing literature is in support of malware training and awareness theme significance for preventing universities’ and colleges' information systems from malware attacks. According to Johnston, Di Gangi, Howard, and Worrell (2019), security training and awareness augments an influence on user behaviors, mitigate risks, and warrants organizational compliance. In alignment, evidence from the study supports the views of Johnson et al concerning the significance of utilizing security training and awareness to deal with personnel issues. Since universities and colleges are a repository of highly sensitive information they serve as an attractive target to cybercriminals. One strategy for enhancing security awareness within an institution is to create a security culture. As noted by da Veiga, Astakhova, Botha, and Herselman (2020), information security culture guide the activities within an institution related to safeguarding data assets while influencing stakeholders’ security perception and behavior. In agreement, gathered data from the study supports the contribution of malware training awareness in creating a security culture within higher education and preventing malware attacks.

Connections to the conceptual model and to other studies. The theme of personnel issues also is in alignment with the general system theory, which is the conceptual framework of this research. Holism is touted as one of the significant principles of the general system theory. According to von Bertalanffy (1968), holism entails the assessment of the system’s state in entirety and not its independent member constituents. As stated by Von Bertalanffy (1968), "all systems have a gestalt, a whole, which cannot be broken down into its constitutional parts and each of the decomposed elements is studied in isolation, but rather one must attempt to view the whole with all its interrelated and interdependent parts in interaction.” Evidence from the study findings recognized personnel as a significant piece of the information security landscape. In alignment, since personnel is part of the whole security system, exclusive analysis and addressing just issues about the user component of the organization without an assessment of its entirety will lead to a security fiasco. This assertion is confirmed in the study findings where three participants claimed malware or data confidentiality threat is not just an IT problem but the entire institution. Thus, addressing malware attacks that threaten the confidentiality of sensitive information in universities’ and colleges’ information system requires the adoption of strategies that considers all aspects of the institution instead of just some sections. Van Assche, Verschraegen, Valentinov, and Gruezmacher (2019) summarizes this view by stating that the system of information security needs to be holistically perceived and not by its constituents parts. Van Assche et al. (2019) claim modifying the system components without taking into consideration the entirety of the system leads to the system’s destruction. In agreement, gathered evidence from the study detests the adoption of strategies that fail to consider all sectors of the university. In the same vein, the general system theory adopts principles that focus on the totality of the system and its interdependencies with sub-systems and systems. Palega and

Knapinski (2018), claim system users as a significant component of an information security system and therefore cannot be separated from the whole system.

An indication from interviewed participants confirms the assertion of personnel as a significant component of the malware prevention security systems. Four out of nine participants presented information that centers all employees, stakeholders, and the entirety of the technology landscape of the institution in the fight against malware attacks. This assertion is confirmed in the words of P4 stating “The human is very critical and cannot be eliminated from the security equation.” Seven out of nine participants similarly reiterated the significant role personnel play in the security process of their respective institutions. As additional evidence, P5 said “our user base is very critical in the malware fight, so we dedicate a lot of resources to educate and train them about the most advanced strategies. Information from the study place system users as significant components of an organization’s security mechanism against malware attacks.

The personnel issues theme based on the findings uncovered during the data analysis stage of the research also aligns with recent studies. Dumitras, Prakash, Subrahmanian, and Wang (2017) in their work about the role of the human factor in successful cyberattacks, stress a positive relationship between the human factor or behavior and malware attacks. Dumitras et al. (2017) further explain that human users are the weakest sources of malware attacks as well as network vulnerabilities. The observations made by Gratian, Bandi, Cukier, Dykstra, and Ginther (2018) confirms the views of Dumitras et al. (2017), who argued that security training and awareness strategies are necessary to resolve data breaches resulting from unwarranted human behaviors. Before this assertion, Gratian et al. (2018) discussed a correlation between certain human characteristics and malware attacks or data breaches within universities and colleges' digital premises. Evidence from Gratian et al. (2018) study depicts the need for IT leaders in universities to prioritize training efforts to system end-users who show some traits that significant indicators of bad security behavior intentions. Findings from the enumerated literature align with the views of study participants as adopting training and awareness programs as preventive controls against malware attacks

Theme 2: Security Planning

Overview. Security planning was the second significant theme to emerge during the data analysis phase of the research. Every higher education institution and its IT department considers its information assets as an integral part of its operation (Bongiovanni, Renaud, & Cairns, 2020). Also, institutional data must be pivotal in the development and implementation of security planning within universities and colleges (Bongiovanni et al., 2020). The theme of security planning is divided into information security policies and procedures subthemes. Information from Table 2 below shows the number of references related to the theme of security planning and subthemes information security policies and procedures.

Table 2

References to Security Planning

Major theme	Participants		Documents	
	Count	References	Count	References
Security planning	9	77	8	9
Subthemes				
Security policies	5	44	8	5
Security procedures	4	33	8	4

Detailed findings from participant interviews and organizational documents.

Information security policies. Evidence from the collected data through the semistructured interviews and institutional documents supports the subtheme of information security policies as one of the significant strategies IT leaders use to prevent malware attacks in universities' and colleges' information systems. To emphasize the contributions of security policies in setting up the rules and practices for all stakeholders accessing and utilizing an organization's resources and assets to comply with, three study participants emphatically expressed the indispensable role it plays in their respective institutions. As noted by P1, "our security policies form the foundation of keeping our systems intact. Without our security policies, our network was influx with serious vulnerabilities." In a similar perspective, P3 stated, "Our security policies dictate how users manage and deal with situations that threaten data integrity. I will say our policies shape us into security-conscious system users." Evidence drawn from the views three other study participants gives credence to the indispensable role of security policies as a bedrock to safeguarding their systems. In alignment, P4 stated, "We don't ever want it to happen here. The reality is it's going to happen. And so having a well-planned, well tested, well thought out procedure and to address it when it does happen is gonna make a world of difference and I have been involved in situations like that where because we had very good policies in place. We cut the problem in half right. By swift action, if we didn't have those policies the problem would have overwhelmed our ability to address it." P4 further presents the fundamental role the institution's security policies play in helping to tackle instances of a data breach. According to P4 "preventing information systems from malware attacks starts with familiarization of the entire data set as well as the associated risks and developing policies and procedures around it. And that's one of the fundamental things that we did, because, at the end of the day, people need to know what has to be protected the most."

As a confirmation, four study participants supported the adoption of policies to guide the conduct of employees and security-related activities, P5 stated "well, we have an institutional manual that addresses codes of conduct, of operating with technology resources which employees are required to familiarize with some sections." Further details from P5 emphasizes the role Bring Your Own Device (BYOD) policies play in shaping how personal devices are used on the network. In the words of P5 "So BYOD is part of what's called a mobile media policy. Any time employees and other network users connect to our network, they are required to abide by the mobile media policy which they are aware of. Meaning employees must ensure their devices are appropriately patched, protect institutional data, and other requirements." To stress the significance of security policies in their respective institution, P6 said "The school has a big school-wide document about the approved and safe practices of both the IT department and other non-tech-savvy staff. The document is pivotal in steering the conduct of all network users." P8 also presented similar perspectives about the implementation of security policies on their premises to ensure the assurance of their systems and their contents. P8 stated, "So we have policies of reporting which are like our reference documents to handle security-related issues."

Information gathered from the perspectives of five study participants shows the adoption of information security policies and procedures as a framework for defending the institutions' systems from malware attacks. As stated by P9 "We have a department manual IT personnel and other employees follow and abide with. The good thing is, our policies are drafted taking into consideration federal regulation compliance." Drawing on the views of P9 and institutional policies about information security has significantly contributed to creating a security culture that foresees the confidentiality of the universities' systems and sensitive contents. Based on gathered information from study participants, Bring Your Own Device (BYOD) security policy, information security policy, encryption standard policy, information handling policy, access control policy, and acceptable user policy are some of the notable policies some universities and colleges' IT department use to manage malware attacks. In the words of participant P4, "preventing information system from malware attacks starts with familiarization of the entire data set as well as the associated risks and developing policies and procedures around it." Inference from the views of P4 reinforces policies as fundamental for malware training and awareness to inform users about what needs to be protected as well as how to achieve that.

Five out of nine study participants claimed malware attacks or data breaches are inevitable, and therefore is imperative for information security professionals to be always ready when it does occur. As a confirmation, P4 stated, “we know we are not immune to malware or any other data breaches, so we are consistently updating our policies and procedures and disaster recovery plans.” To underline the significance of a disaster recovery plan dealing with malware attacks, P5 stated “So I would say that’s the kind of additional information to consider, to have a strong core ecosystem and creating a stronger disaster recovery plan to deal with data breaches.” Participant P4 and P5 recommend the inclusion of effective disaster recovery plans in security policies as an additional layer to protect information systems from malware attacks.

Information gathered from the views of four study participants pinpointed the adoption of effective security policies that take into consideration the institutions’ overall objectives or goals. As stated by participant P2, “cybercriminals are consistently evolving with the intent to launch more sophisticated attacks, hence the need for consistent information security policies to align with the institutions’ to achieve uniformity.” Another thing is cybercriminals are consistently evolving with the intent to launch more sophisticated attacks, hence the need for a consistent update of information security policies to align with the institutions’ to achieve uniformity.” In alignment, P3 stated “the significant trait of our security policies and procedures is the fact that is created with the institution’s main goal in mind. So our policies and procedures are an embodiment of the school's objectives." In the same vein, P6 echoed "Our policies and procedures are not just limited to the IT department but it ties into the school-wide objectives of protecting critical assets." Given the gathered perspectives of the study participants, creating a security policy that aligns with the organization's main objective is critical to establish efficiency and buy-in. Thus, any security policy that fails to accomplish organization objective trait subjects the network to serious vulnerabilities.

Information security policies must be consistently updated to accommodate the explosion of mobile devices on networks as well as the evolving landscape of bad software. P5 confirms with this assertion saying "in response to the explosion of mobile devices in universities' and colleges' network, the IT department through its annual and automatic training, brief all system users and stakeholders with new malware threats while updating policies and procedures to mitigate or neutralize them." As posited by Pathari, and Sonar (2012), the adoption of information security policies to communicate new and existing malware threats helps employees, stakeholders, and the institution as a whole to stay up to date. In agreement, data from the study shows employees are reminded to be cognizant and adhere to all the stipulated guidelines in the information security policies within the educational institution.

All nine study participants concurred the adoption of information security policies in various ways to deal with malware threats. Five out of the nine participants specified gaps in information security are the product of porous information security policies that do not align with the information technology departments' and institution's objectives.

Information security procedures. The findings of the study present information security procedures as a sequence of required steps for performing a specific security task within an institutional or organization setting. Once established, information security procedures set a standard and process for conducting security-related activities within the organization. Five out of the nine study participants expressed the existence of security procedures for executing certain tasks that involve highly sensitive institutional data. P3, stated "one very critical and important thing for security leaders to consider is to establish procedures for doing things such as data backups and retrieval. No data in our network can be transported without following the right encryption procedure." In the same vein, P5 revealed, "I would say we have a guide or a response plan of how to handle confidential data from all systems including legacy systems. We have a flowchart to that effect so that if am out on vacation or somebody else can kind of help under this chart and deal with the situation at hand." P5 further disclosed the adoption of security procedures in dealing with the effective execution of training and awareness programs.

According to the views of four participants, information security procedures are implemented in the form of educating employees about new and trending threats to systems and networks within the organization. In the words of P5 "Again in response to the explosion of mobile devices in universities' and colleges' networks, the IT department through its annual and automatic training, brief all system users and stakeholders with new malware threats while updating policies and procedures to mitigate or neutralize them." P7 added to the contribution of security procedures stating "We have implemented procedures for removing software that is no more in use since hackers take advantage of unused software to get into the system." Three other study participants further disclosed the adoption of security procedures to augment easy data access and in case there is a malware attack. For example, P8 echoed, "As an additional layer for data security and assurance, the IT department has established stringent and meticulously drafted data backups and recovery procedures." The views of P9 were more focused on the existence of procedures for patch management purposes. In the words of P9 "As a department head, one of the things I and the designated staff constantly monitor and follow are the established protocols in the application of patches and updates procedures. Mostly we don't apply security patches right away, we wait until all bugs are fixed."

Drawing on the expressed views of the study participants, information security procedures present the least possible administrative, technical, and physical precautions needed to protect systems and networks from unauthorized access, exposure, and destruction. Five out of the nine study participants expressed the adoption of varied security procedures ranging from patch management, data backup and recovery, vulnerability management, and incidence response which are directed towards preventing universities' and colleges' information systems from malware attacks. Example P5 stated "The most crucial systems are updated monthly with patch updates as they come through. We typically like to stay one version behind on some of those just so we can patch out any bugs and vulnerabilities."

Findings from organizations' documents. Eight institutional documents were collected and analyzed in observing how they support the subthemes of security policies and procedures subthemes. For example, Partner Organization A Document 1 emphatically stated with entrenched guidelines the need for all employees and stakeholders to read and abide by the rules about security training and awareness campaigns. In similar documentation, Partner Organization B Document 2 involves the human resource department to foresee employee and stakeholder compliance with mandatory security training and awareness. Partner Organizations A and B with Documents 3 and 4 respectively presented similar documentation for the performance of backups and the timeframe for the task and related activities to be completed. Partner Organization C Document 5 stipulates the conduct of annual professional development pieces of training with embedded security training and awareness. The content of Document 6 from Partner Organization D further outlines the procedures for data migration from legacy systems to the final destination without subjecting the content to exposure.

Connections to effective information technology practice. The findings of the study are evidence of how information security planning aligns with existing literature. According to Rajab and Eydgahi (2019), the adoption of comprehensive information security planning play a significant role in the protection of an institutions' confidential data and systems from malware attacks. As stated by five study participants, information security planning play a crucial role in foreseeing success in preventing information systems from malware attacks. According to Paliszkiewicz (2019), existing information security models are not comprehensive and consistently managed and updated to reflect changes in policies, risks, and people. This assertion is reflected in the views of four study participants claiming successful malware attacks are a result of institutional failure to effectively manage their assets and strictly apply the rules of its policies. Cybercriminals consistently launch sophisticated malware attacks on universities' and colleges' networks because it's a repository of highly confidential information. Universities' and colleges' information security leaders can minimize malware attacks on their systems by adopting effective communication through training as well as enforcement of its information security policies and procedures (Aurigemma & Mattson, 2017). The findings of the study support the enforcement of security policies and procedures as well as the utilization of security training and awareness campaigns to minimize malware attacks on universities and colleges' information systems which aligns with the views of Aurigemma and Mattson.

Existing literature supports the theme of information security policies and procedures as a strategy universities' and colleges' IT leaders use to prevent malware attacks. As stated by Gashi and Zendeli (2016), information security leaders must ensure the adopted security policies and procedures conforms with established security standards. The indication from the viewpoints of six out of nine study subjects shows routine updates of security policies and procedures to reflect the most recent strategies to nullify trending sophisticated malware types. In the words of Woltjer (2017), higher education institutions must consider a consistent update of information planning mechanisms that reflect modern and effective practices as well as employee and stakeholder compliance. In agreement with Woltjer's idea emphasis on a consistent update of security planning mechanism, indications from the study show a timely update of existing security plans and procedures to reflect modern strategies in dealing with more sophisticated malware or bad software. Six out of nine study participants confirmed the persistent advancement of information technology coupled with its associated convoluted challenges and attacks and therefore confessed utilizing an effective information security plan will partly ensure timely response to malware attacks.

Connections to the conceptual model and other studies. Evidence from study participants plus existing literature supports the theme of information security planning in shaping the perspectives of system users within higher education institutions or organizations. Viewing the theme of information security planning through the lens of general system theory, a higher education institution with effective information security plans will holistically contribute to a secured network environment. In alignment with the holism concept of the general system theory, Barca (2017) stressed any information security system that fails to function in its entirety, results in a breakdown of its defenses. Three out of nine participants claim to deal with malware attacks or data breaches as a whole require a collective effort and that the issue must not be treated as an IT problem but institutional. According to von Bertalanffy (1968), the individual components of the system must function together as a whole to accomplish the main objectives., Adéle (2016) in his work about comparing information security impact on security culture, emphasized the significance of security policies and procedures in building a formidable information security infrastructure and culture within an organization. In this light, since information security planning form an integral part of the security system, an independent assessment, and modification without a holistic analysis will lead to system failure. Five out of the nine study participants confirmed the binding and fundamental role security planning plays in their respective universities or colleges. In the same vein, four out of nine participants claim information security planning that fails to align with the overall higher education institution's security objectives tend to create lapses in the fight against malware attacks and can lead to a possible data breach. As stated by Varsos, Giannakou, and Assimakopoulos (2019), a well-structured security system created through a comprehensive risk-based assessment, considers security planning as pivotal to ensure confidential information assurance.

Existing research also aligns with the theme of information security planning as a strategy to protect information systems from malware attacks. Li et al. (2019) in their work about investigating the impact of security policy and awareness on employees' security behavior, posited a positive relationship between the two. According to Li et al. (2019), when system users are aware of their organizations' information security planning mechanisms, they become more informed about managing situations that threaten information assurance compared to uninformed employees. The responses of four participants align with Li et al. in terms of using training and awareness programs to educate the system users with the necessary tools and skills about their security plans as well as policies and procedures. As stated by Saheb (2013) in his case study about university information security policy. According to Saheb, the existence of information security policies and procedures is critical for a positive reformation on employees' and stakeholders' perceptions of threats to higher education information assets. Similar perspectives are gathered from the study findings in regards to how security policies and procedures have modified the culture of security within the higher education institution. Saheb (2013) noted that, without security planning, employees' security activities about information confidentiality were ethically influenced which varies with individuals. Sohrabi, Von Solms, and Furnell (2016) in similar perspectives discuss that the lack of information security planning, awareness, ignorance, and disregard contributes to the fundamental cause of user security flaws. The consequences of the lack of security policies and procedures according to evidence from the study cause lapses in the security system which aligns with Sohrabi et al.’s perspectives. Employees’ compliance with existing security planning helps to shape and mitigate the threats to institutional data assets linked to employee activities ((Sohrabi et al., 2016).

Theme 3: Security Management Practices

Overview. The third major theme to emerge during the data analysis phase of the study was security management practices. Security management practices entail an assessment of an organization's assets followed by the creation, documentation, and the enactment of policies and procedures to achieve optimum protection. Due to the dynamic and complex nature of the malware landscape, information security leaders must adopt a proactive approach to malware attacks by staying up to date with recent threats, vulnerabilities, and risks. The explosion of mobile and other devices in universities’ and colleges’ networks necessitates the use of appropriate tools and practices to manage these devices. Accordingly, the effective implementation of security management tools and practices can prevent data breaches caused by malware attacks. Table 3 below represents the number of references related to the theme of Security management practices.

Table 3

References to Security Management Tools and Techniques

Major theme	Participant		Documents	
	Count	References	Count	References
Security management practices	8	90	7	8

Findings from participant interviews. Eight out of nine study participants claimed their respective higher education institutions utilized some form of security management practices to protect against malware attacks. In the words of P1 “We have employed both network and host-based intrusion detection technologies like ZScaler, a cloud-based proxy and firewall security tool that helps to route all traffic in and out of our network.” Also, P1 stated, “We remove unused software since the bad guys can exploit this software to gain access to systems.” In the same vein, P2 stated “We have a next-generation anti-malware software installed on all servers and desktop and laptops. That's the first line. We have a vulnerability management program that tracks vulnerabilities and missing updates and patches on all of our important servers, as well as alerts us when there is an issue with our critical systems. We have file integrity monitoring to let us know if critical files have been changed by malware, things like that. We also do traffic monitoring, network traffic monitoring.”

Four out of nine participants confirmed the adoption of security management practices to safeguard their systems from malware attacks, P4 emphasized the utilization of data categorization to help in determining the most critical data and what needs to be protected. In the words of P4 “preventing information systems from malware attacks starts with familiarization of the entire data set as well as the associated risks and developing policies and procedures around it. And that's one of the fundamental things that we did, because, at the end of the day, people need to know what has to be protected the most.” Also, in addition to the adoption of data categorization, P4 stressed the utilization of network segmentation to foster the prevention of universities' and colleges’ information systems from malware attacks. According to P4 “To respond to that, we have something called zero trusts for all students. That means they are treated like any other external internet user. So a lot of organizations are moving to zero trusts. Our systems are designed to only give them access to just their personal information so we don't protect from students any different that we protect from a hacker in Russia or Germany or any other country.” In addition to account management as a strategy to prevent malware infiltration in the system, P4 stated “Like if someone is a temporary employee, we expire their accounts automatically after a certain period or so. So we don’t have to worry if someone forgot to tell us that person is not here, it just turns off because a lot of security problems have been accounts that we call zombies.”

In the technical strategy phase, P5 further presents details that align with the views of other study participants. In the words of P5 “We also have what's called a custom built-in spam filter that blocks out unusual content in systems or the network. So it operates by scanning the network for suspicious emails and most malware attempts or phishing and dormant such activities.” Moreover, P5 further disclosed technical routine tactics like the routine application of patches and backups. In the words of P5 “But the most crucial systems are updated monthly with patch updates as they come through. We typically like to stay one version behind on some of those just so we can patch out any bugs and vulnerabilities. And then the other ones are every other month. So we have a schedule patch site. You know, Microsoft server updates, which is typically the bulk of it that is taking care of those updates. Another is our penetration testing using external contractors and sometimes our team. And it helps us to find openings in the systems and resolve it before it gets out of hand."

P6 presents the utilization of some technical strategies to curb the infiltration of malware or bad software in existing systems and networks. In the words of P6 "We use the protocol Deep Freeze which freezes any computer system attacked by a virus or malware, then after reboot, the attacks are neutralized. Deep Freeze has been very effective to prevent malware attacks on our network. It freezes the drive, freezes everything up but users can still work on the computer." P6 further disclosed the use of third-party vendors like Microsoft cloud services to prevent information systems from malware attacks. According to P6 "We also use Microsoft Office 365, which has cloud-based security that warns us of any unusual security activities and logs it."

Information from the perspectives of five out of the nine participants stressed their respective institutions harnessed the capabilities of third-party security management tools to help prevent malware attacks within their network. Participant P4 claimed the universities' and colleges' IT department utilized network and traffic monitoring tools that augmented the system diagnosis and resolution. As stated by participant P7, "we have adopted both host and network-based intrusion detection technologies like Snort, CrowdsStrike, Falcon, these are cloud-based proxy and firewall security tools."

Four out of nine participants enumerated some notable security tools geared towards the detection, mitigation, and nullification of malware threats to the systems or the entire network as a whole. As stated by P6 “We use a protocol Deep freeze which freezes any computer system attacked by a virus or malware, then after reboot, the attacks are neutralized. Deep freeze has been very effective to prevent malware attacks on our network.”

Findings from organizations’ documents. Also, gathered evidence from some institutional documents in addition to interviewed data during the data analysis phase support the theme of security management practices. Eight of the institutional documents reviewed pinpointed specific tools employed by the IT department to combat malware and other data breach-related attacks. Document 1 from Partner Organization A emphasized the use of state of the art firewall to protect the network from threats to confidential data. In alignment, Document 2 from Partner Organization B disclosed the need for the utilization of email filtering applications to protect the network from the influx of bad software. The usage of data backup strategies and time of plan execution was stipulated in Document 3 from partner organization C. The organizational documents are an embodiment of existing security strategies required to be adopted to prevent information systems from malware attacks. In this light, data from the partner organization confirms the perspectives of study participants.

Connections to effective information technology practice. The perspectives of the study participants about the significance of security management practices align with current literature. Five out of the nine study participants expressed they have implemented some form of security management practices in preventing or mitigating malware attacks in their respective institutions. According to Brunner, Sauerwein, Felderer, and Breu (2020), information security management practices need to be adopted to deal with threats to systems and networks. In alignment, five out of nine study participants reiterated that preventing information systems from malware attacks starts with knowing what needs to be protected coupled with the associated risks and creating policies and procedures to maintain its integrity. As stated by P4 “Preventing information systems from malware attacks starts with familiarization of the entire data set as well as the associated risks and developing policies and procedures around it." Four of the interviewed participants presented a technical outline of the security management practices adopted to ensure the assurance of confidential institutional assets after an evaluation of the potential threats to their assets. As a confirmation P5 stressed “I would say we have a guide or a response plan of how to handle confidential data from all systems including legacy systems. We have a flowchart to that effect so that if am out on vacation a responsible staff can help under this chart and deal with the situation at hand.”

Security management practices empower an organization’s security vision through the formalization of existing infrastructure, the definition of activities, and the application of the required tools and techniques to control, observe and coordinate security efforts within its premise (Pérez-González, Preciado, & Solana-Gonzalez, 2019). The findings from the presented views of four study participants align with that of Pérez-González et al. (2019). According to Fugini, Teimourikia, and Hadjichristofi (2016), cybercriminals have adopted more stealthy and sophisticated methods for deploying malware attacks on targeted systems, hence the need for strategies to combat or mitigate it. Further details from the views of five study participants show information security leaders have resorted to the utilization of some form of modern software or tools for the prevention and mitigation of malware attacks. As stated by Olukoya, Mackenzie, and Omoronyia (2020), information security leaders must be proactive to deal with the heterogeneity and constantly changing scope of malware or bad software in their network premises. To stay up to date with the volatility of the malware landscape, information security leaders should ensure their respective security management practices are constantly updated with the most recent security patches and fixes that align with the institution's goals and objectives. Accordingly, security managers should understand that the institution's data no longer resides in known repositories behind a firewall, hence the need to adopt highly effective security management tools and techniques.

Blythe and Coventry (2018) confirm the need for higher education institutions or organizations to implement some form of security management tools to ensure confidential data residing in the network and systems are free from unauthorized access from both internal and external sources. With the ubiquity and explosion of mobile devices on universities' and colleges' network, it behooves on IT leaders to understand the threat malware or bad software activities pose. In this light, the adoption of effective security tools can go a long way to ensure the security of sensitive system data. During the data analysis, seven organizational documents paved the way for methodological triangulation and established the significance of this theme. Drawing on this, evidence from the study aligns with the most recent literature that fosters the adoption of effective and updated security management practices to accommodate the volatile malware attacks landscape.

Connections to the conceptual model and other studies. The preceding section of the study ties the theme of security management practices to the general system theory which forms the conceptual framework of this study and existing published studies. Van Assche et al. (2019) stated that holism as a fundamental concept of the general system theory stresses an entire assessment of the system components and not through its independent parts. The general systems theory augments the adoption of an integrated approach or an assessment of the relationship between systems (Van Assche et al., 2019). Since security management practices are an important piece to the complex nature of universities' and colleges' technology landscape, the IT department is challenged with managing the numerous components holistically to deal with data security threats. Seven out of the nine participants claimed external data breaches have the most devastating impact on their respective institution's network. As stated by Fucà and Cubico (2020), viewing universities and colleges through the lens of a general system theory brings to light a miscellany of interrelated parts with assigned specific roles working together as a whole to achieve a purpose.

Theme 4: Ethical Hacking

Overview. The final theme to emerge during the data analysis phase of the study is ethical hacking. The concept behind the theme of ethical hacking and simulated attacks relates to a proactive strategy of early vulnerability detection and resolution before malware capitalizes on it. The theme also focuses on legal intrusion into systems and networks to ascertain or measure the robustness of the existing security defense system. According to Cangea (2018), ethical hacking harnesses existing proactive and reactive security techniques to prevent unauthorized intrusion through the discovery and resolution of system vulnerabilities. Evidence from the perspective of study participants coupled with existing literature and institutional documents supports this theme and shows how ethical hacking and simulated attacks can be implemented to prevent information systems from malware attacks. Information from Table 4 below reflects the number of references related to the theme of ethical hacking and simulated attacks.

Table 4

References to Ethical Hacking and Simulated Attacks

Major theme	Participant		Documents	
	Count	References	Count	References
Security management practices	6	72	7	9

Findings from participant interviews and organizational documents. The views of five participants echoed the assertion of harnessing ethical hacking as a proactive and reactive strategy to uncover and resolve system vulnerabilities. Participant P2 stated, “Another thing we have created to proactively prevent malware and other data breach threats is the recent creation of an ethical hacking team responsible to consistently probe the system and network to detect vulnerabilities before cybercriminals do.” In the same vein, participant P4 expressed “Our ethical hacking team is doing a great job to reveal and resolve some most systems and network vulnerabilities before it gets compromised by the bad guys.” P5 further elaborated on the importance of their ethical hacking theme saying “The past two years a bad software compromised one of my systems but was detected early before taking hostage of my network. After that incident, we put together the penetration testing team to help detect and resolve such loopholes ahead of cybercriminals." P6 stated the utilization of external contractors in the early recognition of network loopholes. In the words of P6 "The department sometimes consults the services of third party ethical hackers to help uncover any openings that can be taken advantage of by malware attacks."According to P7, their ethical hacking team strategy has shown positive prospects of safeguarding their network from malware attacks. In the words of P7 "In response to this challenge we have put together an internal ethical hacking team that is constantly probing to discover vulnerabilities before the bad guys do and it has been very efficient." P9 shared the same view about the positive impact of penetration testing strategy. According to P9 "Another recommendation is for universities and colleges to consider the creation of penetration testing teams to probe and assess the robustness of their systems to malware and other data breach attacks."

Five out of the nine participants purported the utilization of penetration testing augments the early detection of suspicious malware activities that prevents cybercriminals from capitalizing on it. For example, P2 stated, "Another thing we have created to proactively prevent malware and other data breach threats is the recent creation of an ethical hacking team responsible to consistently probe the system and network to detect vulnerabilities before cybercriminals do." Six out of the nine participants claimed they have not experienced a malware attack partly because of their ethical hacking strategy which helps in early vulnerability detection and resolution network before escalation. In confirmation, P4 echoed "Our ethical hacking team is doing a great job to reveal and resolve some most systems and network vulnerabilities before it gets compromised by the bad guys. It is one of the contributing reasons why I believe we have not experienced a successful data breach since its adoption."

Three out of six institutional documents analyzed made references to how the ethical hacking team can be tasked to protect confidential data assets from both internal and external malware attacks. Example partner organization A Document 1 stated the need for the ethical team to consistently probe the universities' databases and network using the tools like NMAP and approved modern tools to fortify its defense against malware. In a similar perspective, document 2 from partner organization B further emphasized the need for the IT department to proactively prevent the exposure of institutional systems and contents to unauthorized parties through the use of approved tools. Also, evidence from partner organization C document 3 further reiterates the utilization of ethical services to proactively identify and solve network security flaws. According to Participant P4, "the institution constantly review and update these documents to reflect more efficient ways to deal with evolving and complex malware while ensuring its alignment with institutional objectives." Evidence from the gathered views of study participants coupled with institutional documents supports the theme of ethical hacking as a strategic plan to prevent or mitigate universities' and colleges' information systems from malware attacks.

Connections to effective information technology practice. All study participants concurred successful malware attacks can leave a long-lasting mark on the reputation of the university or college. As posited by O'Neil (2014), data breaches put a dent in both the finances and reputation of colleges that fall victims to successful malware attacks of data breaches. Five out of the nine interviewed subjects concurred the inevitability of malware attacks but agreed to the adoption of proactive strategies to delay and possibly avoid successful threats. A similar notion is presented by Patton (2015) in his work about battling data breaches in higher education institutions. Patton postulated the need for colleges to adopt a proactive security plan to prepare for the inevitable and to promote a security culture. Deducing from the findings of the study, five out of the study participants pinpointed the adoption of ethical hacking tools to help early detection and resolution of system vulnerabilities before being compromised by bad software. The findings of the study about the significance of ethical hacking align with Wallingford, Peshwa, and Kelly (2019) who claim the utilization of ethical hacking or automatic penetration testing effectively minimizes data breach attacks rates and augments a proactive security approach. As opined by Thomas, Burmeister, and Low (2019) organizations should consider the creation of an internal ethical hacking team to provide evidence of reinforcement security investments and to detect known and unknown software and hardware vulnerabilities. Three out of the nine study participants claim their ethical hacking team has fostered early system loophole detection and claimed if the strategy is consistent, their institution may prevent successful malware attacks but not complete immunity. In alignment Cangea (2018) recognized the resiliency of systems and network to bad software when legally probed to uncover vulnerabilities.

Connections to the conceptual model and other studies. The general system theory which formed the conceptual framework of this study aligns with the theme of ethical hacking as a strategy to prevent malware attacks. Universities and colleges that employ ethical hacking to malware attack prevention tend to satisfy a key concept of the general system theory. According to von Bertalanffy (1968), a system is characterized by a miscellany of interrelated and interdependent components that work together to achieve a common goal. To establish optimum security of universities and colleges' networks and systems, IT leaders should consider focusing on all sectors of the institution. P1 and P6 stated the need for an all-inclusive approach to dealing with malware attacks. Five out of nine study participants believed malware prevention is not just an IT problem organization. Six out of nine participants' views align with von Bertallanfy's (1968) general system theory concept of holism. According to Bertallanfy (1968), holism stresses the need to assess a system in its entirety and not through its independent individual components. Drawing on this, universities and colleges' IT leaders may view the institution as a system with varied subsystems working together to achieve a common goal. Aleksandar, Darjan, and Dušan (2019) reiterate that isolating systems into its constituents unites is considered destructive and therefore should not be prioritized. In alignment with the theme of ethical hacking and simulation attacks, the general system can be applied to ensure the strategy takes into consideration all aspects of the institution to be proactive to malware attacks.

According to Fashoto, Ogunleye, and Adabara (2018), penetration testing provides a realistic assessment of security by finding exploits and vulnerabilities inherent in the system or network. Ethical hacking adopts the same principle as hackers to probe into systems to unveil the hidden flaws that can mar the security of a system. Five out of nine study subjects echoed most critical network loopholes that could not have been detected and resolved without the penetration testing service. Evidence from a recent study on how penetration testing can reduce data breach risk, support the claim that to understand how secure a system is, it needs to be subjected to a test (Mansfield-Devine, 2018). Current literature aligns with study findings and supports the theme of ethical hacking and simulated attacks since it stresses the need to subject the systems to test to establish robustness against malware attacks. Mudiyanselage and Pan (2020) posit adopting proactive security is deemed the best approach to deal with malware attacks hence the need for ethical hacking. All study participants align with Mudiyanselage and Pan’s (2020) idea of utilizing a proactive approach to mitigating and preventing malware attacks to stay ahead of cybercriminals. Findings in the above studies encourage the utilization of an ethical hacking approach to security, which aligns with all participants’ responses to the interview questions coupled with the reviewed institutional documents.

Application to Professional Practice

Personnel issue was the first major theme to be discovered during the thematic analysis of the study. Personnel issues pertain to network and system vulnerabilities attributed to user errors and activities. Based on evidence from the findings of the study, personnel issues are effectively addressed through the utilization of security training and awareness programs. Implementing the security training and awareness programs, personnel issues related to security leaders were addressed before it escalates to exposing systems and confidential data to malware attacks. the findings of this study may serve as a great resource to revamp training and awareness programs focused on reducing personnel issues by serving as a great resource. Moreover, the outcomes of the study may serve as an information resource to augment the training of upcoming IT security professionals or leaders. The need for such information is linked to an increasing shortage of information security professionals--projected to hit 1.5 million by the year 2020 (Furnell et al., 2017).

The findings of this study may contribute to the practice of information technology by serving as a repository of information to guide the drafting of stringent security planning, policies, and procedures to combat the threat to systems and networks. Evidence from the study shows misalignment of security planning, policies, and procedures to organizational goals as well as new and evolving threats subject systems and networks to vulnerabilities that can be capitalized on by malware and other forms of bad software. Therefore utilizing the findings of this study may facilitate the designing of security planning strategies that consider the most recent malware trends and data security threats. Drawing on this, efficient and robust information security planning, as well as policies and procedures, may be achieved if the findings of this study are employed. According to Zakarya and Alzamil (2018) security policies and procedures that are consistently updated to reflect the most recent practical and regulatory requirements protect sensitive data from unnecessary data breaches. Also, the study findings would serve as a great resource to IT professionals already in the field in terms of security management practices and rekindle existing strategies for preventing and mitigating malware attacks and for the development of new ones. Hart, Margheri, Paci, and Sassone (2020) in their work stated to bridge the information security skill gap and adopt more stringent strategies IT professionals require access to new and advanced knowledge of mitigating system threats. In a similar discourse, Zeinab (2019) stated some IT professionals lack the ideas in dealing with recent and advanced malware attacks or system threats because of porous and obsolete training and awareness programs that expose them to efficient practices. In the same vein, Aiken (2016) emphasized information security professionals should explore modern and effective strategies and practices that consider and deal with more sophisticated malware attacks. In this light, the findings of the study reveal modern and advanced security management practices such as network security zoning with specific set security requirements to achieve data integrity can be harnessed by information security professionals to mitigate or prevent malware attacks.

Also, the findings of this may contribute to the practice of the information technology profession by serving as a knowledge source for the crafting of proactive strategies for the easy identification and resolution of system vulnerabilities before getting compromised by bad software. Patil, Jangra, Bhale, Raina, and Kulkarni (2017) stated there is an explosion of malware attacks and therefore security professionals should be equipped with some proactive strategies to detect and resolve system loopholes before the cybercriminals do. Patil et al. (2017) posited most security professionals lack the concepts of ethical hacking to foster the optimum system security. In a similar perspective, Yevdokymenko, Mohamed, and Onwuakpa (2017) further elaborated on the effective contributions of ethical hacking in safeguarding systems and networks from unauthorized intrusion. Wallingford et al. (2019) in confirmation, hypothesized the significance of proactive information security strategies, posited the usage of automated penetration testing to effectively diminish and minimize the attack surface and risks. Evidence from the study confirms the contribution of penetration testing in revealing and resolving system and network loopholes before bad software capitalizes on it. Study participants claim their respective ethical hacking teams within the IT department significantly contributed to hardening the systems and network against security threats. In this light, evidence from the study may contribute to IT practice by serving as a great resource for security professionals to acquire knowledge about new tools and procedures for implementing proactive and reactive strategies against malware attacks.

Implications for Social Change

The findings of this study may save universities and college researchers the trauma associated with intellectual property and other study material theft caused by malware attacks. Bad software attacks may disrupt universities' and colleges' academic calendar and research efforts of students and faculty. Such disruptions may result in an additional cost to students in the form of higher fees and other unplanned expenses as well as psychological impacts. According to Al-rimy, Maarof, and Shaid (2018), downtime cost, loss of confidential data, and possible life from malware attacks may negatively impact the conduct of research focused on understanding our society better or solving a problem. The findings of this study may contribute to the society by ensuring the integrity of employees' and students' confidential information as well as saving them from the stress, psychological and social disruption associated with malware attacks. Students and other faculty member are subjected to security threats and safety due to disclose identifies and addresses. As opined by Aiken, Mc Mahon, Haughton, O’Neill, and O’Carroll (2016), the lack of knowledge about the location of personal information as well as closed financial accounts due to compromised social security numbers and health records can significantly increase customers, and other stakeholders’ stress and anxiety levels.

Recommendations for Action

The findings of this study may benefit IT, security leaders, globally by serving as a vital source of information or strategy they can adopt to mitigate or prevent malware attacks. The first recommendation relates to the need for universities’ and colleges’ IT leaders to make a detailed evaluation of the institution’s existing security awareness programs within its premises. As evident from the findings of the study, malware training, and awareness is one of the main strategies security leaders use to prevent malware attacks. Drawing on this, IT security leaders must observe and monitor existing plans for achieving malware awareness to help address vulnerabilities or loopholes. In this light, information security leaders must focus on not only awareness but to also encourage the adoption of creative thinking in the fight against malware attacks.

The second recommendation pertains to the need for security leaders to assess their existing security plans for preventing or mitigating malware attacks and to establish if they align with what is presented in this research. Also, security leaders should consider researching new malware trends coupled with harnessing the expertise of other security professionals in other universities and colleges that may be beneficial to both institutions. Moreover, universities’ and colleges’ IT department without an existing strategy to combat malware attacks should review findings in this study to ascertain its viability to their institution.

The third recommendation is focused on the need for IT leaders to do a comprehensive reevaluation of the existing security management practices for preventing or mitigating malware attacks. This assessment exercise will help to determine if the prevailing security tools are effective in preventing new and existing bad software that threatens the institution's network. Five out of nine participants emphasized the need for security leaders to perform an annual audit of its security management practices within their respective institutions. An annual review or audit of the existing security management tools fosters the adoption of new and improved techniques in fighting against malware threats and the relegation of obsolete ones.

The fourth recommendation is for security leaders to adopt a penetration testing team responsible for performing legal hacking to determine network and system vulnerabilities and to come up with effective solutions. Three out of the nine study participants expressed their respective departments sometimes test stakeholder security awareness through the utilization of simulated attacks and white hat social engineering. In this light, employees that click on simulated emails and social engineering tricks must be further educated about the consequences of real attacks that can result in the theft of highly confidential data. If universities and colleges security leaders follow the enumerated four recommendations, they were confident the adopted information security approach addresses all sectors of the university or college. Also, IT leaders must devise strategies to collect metrics about institutional insiders’ perspectives on existing security training and awareness to foster future modification and accommodation.

Multiple approaches will be utilized in the dissemination of this study's findings. After CAO approval, all study participants will be provided with a summary of my findings. The study will be added to the ProQuest database which is a repository for millions of scholarly journals, newspapers, and reports. Also, I plan to publish my research in other scholarly journals, reports, conferences, and other academic-related publications to increase the chances of reaching the target audience of this study. Also, I will use social media and other educational websites and platforms in reaching the target audience of this research.

Recommendations for Further Research

This study revealed some of the strategies universities’ and colleges’ IT leaders use to prevent and mitigate information systems from malware attacks. Nevertheless, there needs to be further studies about this topic in other industries or organizations that use computer systems in the daily operations and storage of highly confidential information. The study was limited to strategies that universities’ and colleges’ IT leaders in southern California use to prevent malware attacks. In this light, similar studies in different industries in various settings within the United States and other parts of the world are recommended.

The fact that research participants were restricted to only higher education institutions’ IT leaders in southern California, was one of the delimitations that affected this study in terms of generalization of findings to other industries and settings. In this regard, this research may be replicated in other industries and organizations to ascertain its extensive applicability.

One notable assumption of this study was that study subjects will honestly respond to study questions. Due to the sensitivity, confidentiality, and organizational requirements, some study participants were reluctant to present some information until they were assured of personality anonymity. Protecting study participants from identity disclosure contributed to the gathering of rich data to help answer the overarching question.

Also, using a different research approach or design like quantitative may provide an additional perspective about malware attacks. For example, using a quantitative study to assess the impact or the relationship between malware training and awareness and possible data breaches. This type of study could help evaluate the impact of malware training and awareness in preventing data breaches and attacks within a university or an organization setting. Although this study has contributed to the literature, further research about malware attacks in other industries can be advantageous to the information security industry.

Reflections

In my quest to explore strategies utilized by universities and colleges' IT leaders to prevent and mitigate information systems from malware attacks, I observed the complex nature of the bad software that threatens confidentiality coupled with existing strategies to combat the risks. This study was one of the most challenging academic undertakings of my life. The study has impacted my perspective on the conduct of academic research and has increased my respect for anyone trying or has attained the doctoral title. To contribute to the credibility of this study especially amid the coronavirus pandemic, I utilized techniques to prevent and minimize personal bias from determining the direction of the research. I strictly adhered to the tenets of the interview protocol with all study participants coupled with a provision of opportunity to verify the authenticity of gathered information through member checking sessions. Using the interview protocol as a guide, I was cognizant of my body language during the video interview to avoid triggering perceptions that might result in research bias. Also, I avoided having predetermined thoughts because of the environmental parameters as well as maintained a neutral body composure, a facial expression that might result in bias from the respondent. I asked questions without offering a personal opinion and data responses were gathered devoid of preconceived notion interruptions. The organizational documents, interview data, and member checking were also used to establish triangulation in this study.

Although there were unforeseen challenges like the COVID 19 pandemic, some positive outcomes were observed during the research process. The first is about how participants were willing to share their experiences about strategies utilized to prevent malware attacks to support the research considering the challenge with virtual delivery of academic instruction due to the pandemic. The second relates to joy and excitement to have finally completed this study and to decide on the way forward.

Conclusion

Since the 1970s, the evolution of malware continues to exhibit a complex trajectory and therefore advanced and more complicated remediation strategies must be adopted to mitigate or prevent this menace. Information technology leaders need to revamp programs and strategies to address and reshape user activities coupled with the adoption of security policies and procedures on how to manage malware-related threats, may significantly help mitigate the proliferation of malware attacks in universities' and colleges' systems and networks. As opined by Hatfield (2019), security leaders must understand that malware attacks are inevitable and are constantly evolving, therefore preventive and mitigating strategies must be updated with new intelligence to deal with the threat.

References

Abdalla, M. M., Oliveira, L. G. L., Azevedo, C. E. F., & Gonzalez, R. K. (2018). Quality in qualitative organizational research: Types of triangulation as a methodological alternative. *Administração: Ensino e Pesquisa*, *19*(1), 66–98. doi:10.13058/raep.2018.v19n1.578

Abellán, J. I. M. (2019). Hopscotch 2.0: An enhanced version of the model for the generation of research designs in social sciences and education. *Georgia Educational Researcher*, *16*(1), 5–22. Retrieved from https://digitalcommons.georgiasouthern.edu/gerjournal/

Adams, C. (2018). Learning the lessons of WannaCry. *Computer Fraud & Security*, *2018*(9), 6–9. doi:10.1016/S1361-3723(18)30084-8

Adéle, D. V. (2016). Comparing the information security culture of employees who had read the information security policy and those who had not: Illustrated through an empirical study. *Information & Computer Security*, *24*(2), 139–151. doi:10.1108/ICS-12-2015-0048

Adkoli, B., & Parija, S. (2019). Systems approach in medical education: The thesis, antithesis, and synthesis. *Tropical Parasitology*, *9*(1), 3–6. doi:10.4103/tp.TP_7_19

Adu, K. K., & Adjei, E. (2018). The phenomenon of data loss and cybersecurity issues in Ghana. *Foresight*, *20*(2), 150–161. doi:10.1108/FS-08-2017-0043

Aiken, M., Mc Mahon, C., Haughton, C., O'Neill, L., & O'Carroll, E. (2016). A consideration of the social impact of cybercrime: examples from hacking, piracy, and child abuse material online. *Contemporary Social Science*, *11*(4), 373–391. doi:10.1080/21582041.2015.1117648

Alajlouni, B. A. (2017). Exploring the potential of the innate immune system for computers network security. *International Journal of Computer Science Issues*, *14*(2), 24–29. doi:10.20943/01201702.2429

Alase, A. (2017). The interpretative phenomenological analysis (IPA): A guide to a good qualitative research approach. *International Journal of Education and Literacy Studies*, *5*(2), 9–19. Retrieved from https://www.journals.aiac.org.au/index.php/IJELS

Albahar, M. (2019). Cyber attacks and terrorism: A twenty-first century conundrum. *Science and Engineering Ethics*, *25*(4), 993–1006. doi:10.1007/s11948-016-9864-0

Aldawood, H., & Skinner, G. (2019). Reviewing cyber security social engineering training and awareness programs—Pitfalls and ongoing issues. *Future Internet*, *11*(3), 73. Retrieved from https://www.mdpi.com/journal/futureinternet

Aleksandar, S., Darjan, K., & Dušan, R. (2019). The importance of the general system theory for the modern world. *Trendovi u Poslovanju*, *7*(2), 87–94. Retrieved from http://trendovi.indmanager.org/index.php/tp

AlHarrasi, N. (2016). Using soft systems methodology in social sciences: Improvement of the research methods module at the Department of Information Studies at Sultan Qaboos University as an example. *Journal of Arts and Social Sciences*, *7(*3), 5–15. doi: 10.24200/jass.vol7iss3pp5-15

Al-rimy, B. A. S., Maarof, M. A., & Shaid, S. Z. M. (2018). Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions. *Computers & Security*, *74*, 144–166. doi:10.1016/j.cose.2018.01.001

Amankwaa, L. (2016). Creating protocols for trustworthiness in qualitative research. *Journal of Cultural Diversity*, *23*(3), 121–127. Retrieved from http://tuckerpub.com/jcd.htm

Amundsen, D., Msoroka, M., & Findsen, B. (2017). “It’s a case of access”: The problematics of accessing research participants. *Waikato Journal of Education*, 22(4), 5–17. doi:10.15663/wje.v22i4.425

Anderson, V. (2017). Criteria for evaluating qualitative research. *Human Resource Development Quarterly*, *28*(2), 125–133. doi:10.1002/hrdq.21282

Andrei, T. (2018). The Internet—Secondary data source in marketing research. *Annals of “Constantin Brancusi” University of Targu-Jiu—Economy Series*, (6), 92–97. Retrieved from https://ideas.repec.org/s/cbu/jrnlec.html

Anselmi, P., Fabbris, L., Martini, M. C., & Robusto, E. (2018). Comparison of four common data collection techniques to elicit preferences. *Quality & Quantity*, 52(3), 1227–1239. doi:10.1007/s11135-017-0514-7

Armstrong, C. S., & Kepler, J. D. (2018). Theory, research design assumptions, and causal inferences. *Journal of Accounting and Economics*, *66*(2–3), 366–373. doi:10.1016/j.jacceco.2018.08.012

Aurangzeb, S., Aleem, M., Iqbal, M. A., & Islam, M. A. (2017). Ransomware: A survey and trends. *Journal of Information Assurance & Security*, *6*(2), 48–58. Retrieved from https://www.mirlabs.net/iasl/

Aurigemma, S., & Mattson, T. (2017). Privilege or procedure: Evaluating the effect of employee status on intent to comply with socially interactive information security threats and controls. *Computers & Security*, *66*, 218–234. doi:10.1016/j.cose.2017.02.006

Aytac, V. (2019). Vulnerability in networks. *Journal of Applied and Engineering Mathematics*, (2), 366. Retrieved from http://jaem.isikun.edu.tr/web/

Banathy, B. H. (1991). *Systems Design of Education: A Journey to Create the Future*. Englewood Cliffs, N.J.: Educational Technology Publications.

Barca, D. C. (2017). Information security in digital trunking systems. *Database Systems Journal*, *8*(1), 40–48. Retrieved from http://www.dbjournal.ro/

Baškarada, S., & Koronios, A. (2018). A philosophical discussion of qualitative, quantitative, and mixed methods research in social science. *Qualitative Research Journal*, (1), 2. doi:10.1108/QRJ-D-17-00042

Belotto, M. J. (2018). Data analysis methods for qualitative research: managing the challenges of coding, interrater reliability, and thematic analysis. *Revista Brasileira de Enfermagem*, *71*, 2622–2633. Retrieved from https://www.scielo.br/scielo.php?script=sci_serial&pid=0034-7167

Ben-Hador, B. (2016). Coaching executives as tacit performance evaluation: A multiple case study. *Journal of Management Development*, *35*(1), 75-88. doi: 10.1108/JMD-08-2014-0091

Benoot, C., Hannes, K., & Bilsen, J. (2016). The use of purposeful sampling in a qualitative evidence synthesis: A worked example on sexual adjustment to a cancer trajectory. *BMC Medical Research Methodology*, *16*(1), 1–12. doi:10.1186/s12874-016-0114-6

Birt, L., Scott, S., Cavers, D., Campbell, C., & Walter, F. (2016). Member checking: A tool to enhance trustworthiness or merely a nod to validation? *Qualitative Health Research*, *26*(13), 1802–1811. doi:10.1177/1049732316654870

Black, P., Gondal, I., & Layton, R. (2018). A survey of similarities in banking malware behaviours. *Computers & Security*, (77), 756–772. doi: 10.1016/j.cose.2017.09.013

Blaikie, N. (2018). Confounding issues related to determining sample size in qualitative research. *International Journal of Social Research Methodology, 21*(5), 635–641. doi:10.1080/13645579.2018.1454644

Bleiker, J., Morgan-Trimmer, S., Knapp, K., & Hopkins, S. (2019). Navigating the maze: Qualitative research methodologies and their philosophical foundations. *Radiography*, *25*(1), S4–S8. doi: 10.1016/j.radi.2019.06.008

Bloomfield, J., & Fisher, M. J. (2019). Quantitative research design. *Journal of the Australasian Rehabilitation Nurses' Association (JARNA)*, *22*(2), 27–30. doi:10.33235/jarna.22.2.27-30

Blythe, M. J., & Coventry, L. (2018). Costly but effective: Comparing the factors that influence employee anti-malware behaviours. *Computers in Human Behavior, 87,*87-97. doi:10.1016/j.chb.2018.05.023.

Boddy, C. R. (2016). Sample size for qualitative research. *Qualitative Market Research:*

An International Journal, *19*(4), 426–432. doi:10.1108/QMR-06-2016-0053

Bongiovanni, I. (2019). The least secure places in the universe? A systematic literature review on information security management in higher education. *Computers & Security*, *86*, 350–357. doi: 10.1016/j.cose.2019.07.003

Bongiovanni, I., Renaud, K., & Cairns, G. (2020). Securing intellectual capital: an exploratory study in Australian universities. *Journal of Intellectual Capital*, *21*(3), 481–505. doi:10.1108/JIC-08-2019-0197.

Borgman, L. C. (2018). Open data, grey data, and stewardship: Universities at the privacy frontier. *Berkeley Technology Law Journal*, *33*(2), 365-412. doi: 10.15779/Z38B56D489

Borislav, V. (2016). Research design: qualitative, quantitative, and mixed methods approaches London: Sage publications, 2009. *Politeia*, *6*(12), 191-194. Retrieved from http://www.doaj.org/

Bowdich, D. (2018). State sponsored cyber theft: Nine Iranians charged massive campaign on behalf of Iran government. Retrieved from http://www.fbi.gov

Bridgen, S. (2017). Using systems theory to understand the identity of academic advising: A case study. *NACADA Journal*, *37*(2), 9–20. doi:10.12930/NACADA-15-038

Bronstein, M. V., Pennycook, G., Joormann, J., Corlett, P. R., & Cannon, T. D. (2019). Dual-process theory, conflict processing, and delusional belief. *Clinical Psychology Review*, 72. doi: 10.1016/j.cpr.2019.101748

Brown, A., & Danaher, P. A. (2019). CHE Principles: Facilitating authentic and dialogical semistructured interviews in educational research. *International Journal of Research & Method in Education*, *42*(1), 76–90. Retrieved from https://www.ebscohost.com/

Brown, H. (2016). After the data breach: Management the crisis and mitigating the impact. *Journal of Business Continuity & Emergency Planning*, *9*(4), 317-328. Retrieved from http://www.henrystewartpublications.com/

Brunner, M., Sauerwein, C., Felderer, M., & Breu, R. (2020). Risk management practices in information security: Exploring the status quo in the DACH region. *Computers & Security*, *92*. doi:10.1016/j.cose.2020.101776

Buetow, S. (2019). Apophenia, unconscious bias and reflexivity in nursing qualitative research. *International Journal of Nursing Studies*. doi: 10.1016/j.ijnurstu.2018.09.013

Butler, D., Leahy, M., Twining, P., Akoh, B., Chtouki, Y., Farshadnia, S., … Valtonen, T. (2018). Education systems in the digital age: The need for alignment. *Technology, Knowledge and Learning*, *23*(3), 473–494. Retrieved from https://www.ebscohost.com/

Cangea, O. (2018). Ethical hacking solution to defeat cyber attacks. *Petroleum - Gas University of Ploiesti Bulletin, Technical Series*, *70*(2), 29–36. Retrieved from http://www.bulletin.upg-ploiesti.ro/

Carminati, L. l. (2018). Generalizability in qualitative research: A tale of two traditions. *Qualitative Health Research*, *28*(13), 2094–2101.

doi:10.1177/1049732318788379

Carr, E. M., Zhang, G. D., Ming, J., Hung, Y., & Siddiqui, Z. S. (2019). Qualitative research: An overview of emerging approaches for data collection. *Australasian Psychiatry*, *27*(3), 307–309. doi:10.1177/1039856219828164

Castillo-Montoya, M. (2016). Preparing for interview research: The interview protocol refinement framework. *The Qualitative Report*, *21*(5), 811-831. Retrieved from https://www.nsuworks.nova.edu/tqr/vol21/iss5/2

Castleberry, A., & Nolen, A. (2018). Thematic analysis of qualitative research data: Is it as easy as it sounds? *Currents in Pharmacy Teaching and Learning*, *10*(6), 807–815. doi: 10.1016/j.cptl.2018.03.019

Cataldi, S. (2018). A proposal for the analysis of the relational dimension in the interview techniques: A pilot study on in-depth interviews and focus groups. *Quality & Quantity*, *53*(1), 295-312. doi:10.1007/s11135-017-0468-9

Cathcart, A. (2019). The secret war for china: espionage, revolution and the rise of mao. *War in History*, *26*(2), 300–302. doi:10.1177/0968344518804624c

Chandrasekar, C., & Priyatharsini, P. (2018). Classification techniques using spam filtering email. *International Journal of Advanced Research in Computer Science*, *9*(2), 402. Retrieved from http://journaldatabase.info/journal/issn0976-5697

Checkland, P. (2000). Soft systems methodology: A thirty-year retrospective(a). *Systems Research and Behavioral Science*. Retrieved from https://www.wiley.com/en-us

Chen, H., Su, J., Qiao, L., & Xin, Q. (2018). Malware collusion attack against SVM:

Issues and countermeasures. *Applied Sciences-Basel*, *8*(10). doi:10.3390/app8101718

Chmura, J. (2017). Forming the awareness of employees in the field of information security. *Journal of Positive Management*, *8*(1), 78. Retrieved from https://apcz.umk.pl/czasopisma/index.php/JPM

Choi, S., Martins, J. T., & Bernik, I. (2018). Information security: Listening to the perspective of organisational insiders. *Journal of Information Science*, *44*(6), 752–767. doi:10.1177/0165551517748288

Christensen, K. K., & Liebetrau, T. (2019). A new role for “the public”? Exploring cyber security controversies in the case of WannaCry. *Intelligence & National Security*, *34*(3), 395–408. doi:10.1080/02684527.2019.1553704

Clark, K. R., & Vealé, B. L. (2018). Strategies to enhance data collection and analysis in qualitative research. *Radiologic Technology*, *89*(5), 482CT–485CT. Retrieved from http://www.radiologictechnology.org/

Clark, L., Birkhead, A. S., Fernandez, C., & Egger, M. J. (2017). A transcription and translation protocol for sensitive cross-cultural team research. *Qualitative Health Research*, *27*(12), 1751–1764. doi:10.1177/1049732317726761

Collingridge, D. S., & Gantt, E. E. (2019). The quality of qualitative research. *American Journal of Medical Quality*, *34*(5), 439. Retrieved from https://us.sagepub.com/en-us/nam

Connelly, L. M. (2016). Understanding research. Trustworthiness in qualitative research. *MEDSURG Nursing*, *25*(6), 435–436. Retrieved from http://www.medsurgnursing.net/cgi-bin/WebObjects/MSNJournal.woa

Corneanu, S. (2017). Bacon and the government of knowledge. Critique, invention, system: modern thinking as a proof of history. *Renaissance Quarterly, 70*(4), 1491–1492. Retrieved from https://www.jstor.org/journal/renaquar

Craig, J. M. (2019). Extending situational action theory to white-collar crime. *Deviant Behavior*, 40(2), 171–186. doi:10.1080/01639625.2017.1420444

Curry, J., & Drage, N. (2017). IoT: The internal and external threat. *IT Now*, *59*(1), 30–31. doi:10.1093/itnow/bwx014

Cypress, B. (2018). Qualitative research methods: A phenomenological focus. *Dimensions of Critical Care Nursing*, *37*(6), 302–309. doi: 10.1097/DCC.0000000000000322

da Veiga, A., Astakhova, L. V., Botha, A., & Herselman, M. (2020). Defining organisational information security culture—Perspectives from academia and industry. *Computers & Security, 92*. doi:10.1016/j.cose.2020.101713

De Simone, D. M. (2019). Data breaches are not just information technology worries! *Pediatric Nursing*, *45*(2), 59–62. Retrieved from http://www.pediatricnursing.net/

DeCino, D. A., & Waalkes, P. L. (2019). Aligning epistemology with member checks. *International Journal of Research & Method in Education*, *42*(4), 374–384. doi:10.1080/1743727X.2018.1492535

Demetis, D. S. (2018). Fighting money laundering with technology: A case study of Bank X in the UK. *Decision Support Systems*, *105*, 96–107. doi:

10.1016/j.dss.2017.11.005.

Deng, J. (1982). Grey systems control. *Systems & Control Letters*, 1, 288-294. doi: 10.1016/S0167-9611(82)80025-X

Department of Justice (DOJ). (2018). report. Two Iranian men indicted for deploying ransomware to extort hospitals, municipalities, and public institutions, causing over $30 million in losses. Retrieved from http://www.justice.gov

Derouet, E. (2016). Fighting phishing and securing data with email authentication. *Computer Fraud & Security*, *2016*(10), 5–8. doi:10.1016/S1361-3723(16)30079-3

Dhukaram, A. V., Sgouropoulou, C., Feldman, G., & Amini, A. (2018). Higher education provision using systems thinking approach--case studies. *European Journal of Engineering Education*, *43*(1), 3–25. doi:10.1080/03043797.2016.1210569

Ding, Y., Wu, R., & Zhang, X. (2019). Ontology-based knowledge representation for malware individuals and families. *Computers & Security*, *87*. doi:10.1016/j.cose.2019.101574

Dumitras, T., Prakash, B. A., Subrahmanian, V. S., & Wang, B. (2017). Understanding the relationship between human behavior and susceptibility to cyber attacks. *ACM Transactions on Intelligent Systems & Technology*, *8*(4), 1–25. doi:10.1145/2890509

Edmonds, E. A. (2017). General system theory: Foundations, development, applications by Ludwig von Bertalanffy (review), *Leonardo & Leonardo Music Journal,* 3 248. Retrieved from https://muse-jhu-edu.ezp

Ellis, P. (2019). Ethical aspects of research. *Wounds UK, 15*(3), 87–88. Retrieved from https://www.wounds-uk.com/

Espinosa, J. A., Davis, D., Stock, J., & Monahan, L. (2019). Exploring the processing of product returns from a complex adaptive system perspective. *The International Journal of Logistics Management*, 30(3), 699–722. doi:10.1108/IJLM-08-2018-0216.

Fashoto, S. G., Ogunleye, G. O., & Adabara, I. (2018). Evaluation of network and systems security using penetration testing in a simulation environment. *Computer Science & Telecommunications, 55*(3), 3–12. Retrieved from https://www.ijcst.org/

Federal Bureau of Investigation Internet Crime Complaint Center (IC3). (2018). 2018 report. Retrieved from http://www.fbi.gov/

Feng, C., & Wang, T. (2019). Does CIO risk appetite matter? Evidence from information security breach incidents. *International Journal of Accounting Information Systems*, *32*, 59–75. doi: 10.1016/j.accinf.2018.11.001

Ferrando, M., Hoogerwerf, E., & Kadyrbaeva, A. (2019). Qualitative research on the factors affecting transferability of digital solutions for integrated care. *International Journal of Integrated Care, 19*(4), 1-8. doi:10.5334/ijic.s3236

Fidler, B. (2017). Cybersecurity governance: A prehistory and its implications. *Digital Policy, Regulation and Governance, 19*(6), 449-465. doi:10.1108/DPRG-05-2017-0026

FitzPatrick, B. (2019). Validity in qualitative health education research. *Currents in*

Pharmacy Teaching & Learning, 11(2), 211–217. doi: 10.1016/j.cptl.2018.11.014

Forero, R., Nahidi, S., De Costa, J., Mohsin, M., Fitzgerald, G., Gibson, N., … Aboagye-Sarfo, P. (2018). Application of four-dimension criteria to assess rigour of qualitative research in emergency medicine. *BMC Health Services Research, 18*(1), 1-11. doi:10.1186/s12913-018-2915-2

Friesen, P., Kearns, L., Redman, B., & Caplan, A. L. (2017). Rethinking the Belmont Report? *American Journal of Bioethics*, *17*(7), 15–21. doi:10.1080/15265161.2017.1329482

Fucà, R., & Cubico, S. (2020). Undecidability and the evolution of ideas in an emergency event: An example of how to systemically test organizational effectiveness (OE) in university groups. *Education Sciences*, *10*(135), 135. doi:10.3390/educsci10050135

Fugini, M., Teimourikia, M., & Hadjichristofi, G. (2016). A web-based cooperative tool for risk management with adaptive security. *Future Generation Computer Systems*, *54*, 409–422. doi:10.1016/j.future.2015.04.015

Furnell, S., Fischer, P., & Finch, A. (2017). Feature: Can't get the staff? The growing need for cyber-security skills. *Computer Fraud & Security*, *2017*(2), 5–10. doi:10.1016/S1361-3723(17)30013-1

Fusch, P., Fusch, G. E., & Ness, L. R. (2018). Denzin's paradigm shift: Revisiting triangulation in qualitative research. *Journal of Social Change, 10*(1), 19–32. doi:10.5590/JOSC.2018.10.1.02

Gaisina, L. M., Belonozhko, M. L., Artyukhov, V. A., Sultanova, E. A., & Dallakian, G.

R. (2017). The organization as a social self-governing system. *Journal of Advanced Research in Law and Economics,*2(24),454 – 462. doi: 10.14505/jarle.v8.2(24).14

Galdas, P. (2017). Revisiting bias in qualitative research. *International Journal of Qualitative Methods*. 16,1-2. doi:10.1177/1609406917748992

Gashi, B., & Zendeli, F. (2016). The impact of security and intelligence policy in the era of cyber crimes. *ILIRIA International Review, 6*(1), 157–164. doi:10.21113/iir.v6i1.211

Gastil, R. D. (1975). Kuhn’s “the logic of social systems”: The rational first approximation as social science. *Policy Sciences*, *6*(4), 467–479. doi:10.1007/BF00142385

Gauchi, R. V. (2017). Study of the research methods and data collection techniques used in library and information science. *Revista Espanola De Documentacion Cientifica*, *40*(2). doi:10.3989/redc.2017.2.1333

Gentles, J. S., Charles, C., Nicholas, B. D., Ploeg, J., & McKibbon, A. K. (2016). Reviewing the research methods literature: Principles and strategies illustrated by a systematic overview of sampling in qualitative research. *Systematic Reviews,* *5*(172), 1-11. doi: 10.1186/s13643-016-0343-0

Giudici, A., Reinmoeller, P., & Ravasi, D. (2018). Open-system orchestration as a relational source of sensing capabilities: Evidence from a venture association. *Academy of Management Journal*, *61*(4), 1369–1402. doi:10.5465/amj.2015.0573

Glenna, L., Hesse, A., Hossain, N., & Scott-Villiers, P. (2019). Ethical and methodological issues in large qualitative participatory studies. *American Behavioral Scientist*, *63*(5), 584–603. doi:10.1177/0002764218775782

Goode, S., Hoehle, H., Venkatesh, V., & Brown, S. A. (2017). User compensation as a data breach recovery action: An investigation of the Sony PlayStation network breach. *MIS Quarterly*, *41*(3), 703-A16. Retrieved from https://www.misq.org/

Gratian, M., Bandi, S., Cukier, M., Dykstra, J., & Ginther, A. (2018). Correlating human traits and cyber securi Anwar,ty behavior intentions. *Computers & Security, 73*, 345–358. doi:10.1016/j.cose.2017.11.015

Greenaway, K. H., & Cruwys, T. (2019). The source model of group threat: Responding to internal and external threats. *American Psychologist*, *74*(2), 218–231. doi:10.1037/amp0000321

Grimes, P. E. (2017). Evolution and world-systems: Complexity, energy, and form. *Journal of World-Systems Research*, 23(2), 678. Retrieved from https://www.ebscohost.com/

Grysman, A., & Lodi-Smith, J. (2019). Methods for conducting and publishing narrative research with undergraduates. *Frontiers in Psychology*. doi:10.3389/fpsyg.2018.02771

Guo, H., Cheng, H. K., & Kelley, K. (2016). Impact of network structure on malware propagation: A growth curve perspective. *Journal of Management Information Systems*, *33*(1), 296–325. doi:10.1080/07421222.2016.1172440

Gwebu, K. L., Wang, J., & Wang, L. (2018). The role of corporate reputation and crisis response strategies in data breach management. *Journal of Management Information Systems*, *35*(2), 683–714. doi:10.1080/07421222.2018.1451962

Hadi, M. A., & Closs, S. J. (2016). Ensuring rigour and trustworthiness of qualitative research in clinical pharmacy. *International Journal of Clinical Pharmacy*, *38*(3), 641-646. doi:10.1007/s11096-015-0237-6

Hagen, M. J., Albrechtsen, E., & Hovden, J. (2008). Implementation and effectiveness of organizational information security measures. *Information Management & Computer Security*, *16*(4), 377–397. doi:10.1108/09685220810908796

Hamilton, G., Powell, M. B., & Brubacher, S. P. (2017). Professionals' perceptions regarding the suitability of investigative interview protocols with aboriginal children. *Australian Psychologist*, *52*(3), 174-183. Retrieved from https://www.psychology.org.au/

Hammouchi, H., Cherqi, O., Mezzour, G., Ghogho, M., & Koutbi, M. E. (2019). Digging deeper into data breaches: an exploratory data analysis of hacking breaches over time. *Procedia Computer Science*, 171, 1004–1009. doi: 10.1016/j.procs.2019.04.141

Hancock, M. E., Amankwaa, L., Revell, M. A., & Mueller, D. (2016). Focus group data saturation: a new approach to data analysis. *Qualitative Report*, *21*(11), 2124-2130. Retrieved from https://nsuworks.nova.edu/tqr/

Haqaf, H., & Koyuncu, M. (2018). Understanding key skills for information security managers. *International Journal of Information Management*, *43*, 165–172. doi:10.1016/j.ijinfomgt.2018.07.013

Hart, S., Margheri, A., Paci, F., & Sassone, V. (2020). Riskio: A serious game for cyber security awareness and education. *Computers & Security*, *95*, 1-16 .doi:10.1016/j.cose.2020.101827

Hartblay, C. (2018). This is not thick description: Conceptual art installation as ethnographic process. *Ethnography*, *19*(2), 153–182. doi:10.1177/1466138117726191

Hatfield, J. M. (2018). Social engineering in cybersecurity: The evolution of a concept. *Computers & Security*, *73*(2018), 102–113. doi:10.1016/j.cose.2017.10.008

Hatfield, J. M. (2019). Virtuous human hacking: The ethics of social engineering in penetration-testing. *Computers & Security*, *83*(2019), 354–366. doi:10.1016/j.cose.2019.02.012

Herrera-Restrepo, O., & Triantis, K. (2019). Enterprise design through complex adaptive systems and efficiency measurement. *European Journal of Operational Research*, *278*(2), 481-497. doi: 10.1016/j.ejor.2018.12.002.

Hina, S., & Dominic, P. D. D. (2020). Information security policies' compliance: a perspective for higher education institutions. *Journal of Computer Information Systems*, *60*(3), 201–211. doi:10.1080/08874417.2018.1432996

Hodiamont, F., Jünger, S., Leidl, R., Maier, O. B., Schildmann, E., & Bausewein, C. (2019). Understanding complexity – the palliative care situation as a complex adaptive system. *BMC Health Services Research*, *19*(1), 1-14. doi:10.1186/s12913-019-3961-0

Holt, N. L., & McHugh, T.-L. (2018). A critical evaluation of three member-checking procedures. *International Journal of Qualitative Methods*, 17(1). Retrieved from https://www.ebscohost.com/

Horne, A. C., Maynard, S. B., & Ahmad, A. (2017). Organizational information security strategy: review, discussion and future research. *Australasian Journal of Information Systems*, *21*,1-17. doi:10.3127/ajis.v21i0.1427

Horner, M., & Hyslip, T. (2017). SQL Injection: The longest running sequel in programming history. *Journal of Digital Forensics, Security & Law, 12*(2), 97–108. Retrieved from https://www.jdfsl.org/

Howard, L. C., & Hammond, S. P. (2019). Researcher vulnerability: Implications for educational research and practice. *International Journal of Qualitative Studies in Education (QSE), 32*(4), 411-428. doi:10.1080/09518398.2019.1597205

Hryshchuk, R., & Yevseiev, S. (2016). The synergetic approach for providing bank information security: The problem formulation. *Ukrainian Scientific Journal of Information Security*, *22*(1), 64–74. doi:10.18372/2225-5036.22.10456

Ingold, P. V., Donni, M., & Lievens, F. (2018). A dual-process theory perspective to better understand judgments in assessment centers: The role of initial impressions for dimension ratings and validity. *Journal Of Applied Psychology*, 103(12), 1367–1378. doi:10.1037/apl0000333.

Jaeger, L., Eckhardt, A., & Kroenung, J. (2020). The role of deterrability for the effect of multi-level sanctions on information security policy compliance: Results of a multigroup analysis. *Information & Management,1*-14 doi:10.1016/j.im.2020.103318

Jaf, S., Ghafir, I., Prenosil, V., Saleem, J., Hammoudeh, M., Faour, H., ...& Baker, T. (2018). Security threats to critical infrastructure: the human factor. *Journal of Supercomputing*, *74*(10), 4986–5002. doi:10.1007/s11227-018-2337-2

Jamali, H. R. (2018). Does research using qualitative methods (grounded theory, ethnography, and phenomenology) have more impact? *Library and Information Science Research*, *40*(3–4), 201–207. doi: 10.1016/j.lisr.2018.09.002

Jensen, M. L., Dinger, M., Wright, R. T., & Thatcher, J. B. (2017). Training to mitigate phishing attacks using mindfulness techniques. *Journal of Management Information Systems*, *34*(2), 597–626. doi:10.1080/07421222.2017.1334499

Jeong, C. Y., Lee, S. Y. T., & Lim, J. H. (2018). Information security breaches and IT security investments: Impacts on competitors. *Information & Management*, *56*(5), 681-695. doi:10.1016/j.im.2018.11.003

Johnson, B., Holness, K., Porter, W., & Hernandez, A. (2018). Complex adaptive systems of systems: A grounded theory approach. *Grounded Theory Review*, *7*(1), 52–69. Retrieved from http://groundedtheoryreview.com/

Johnston, A. C., Di Gangi, P. M., Howard, J., & Worrell, J. (2019). It takes a village: Understanding the collective security efficacy of employee groups. *Journal of the Association for Information Systems*, *20*(3), 186–212. doi:10.17705/1jais.00533

Jordan, K. (2018). Validity, reliability, and the case for participant-centered research: Reflections on a multi-platform social media study. *International Journal of*

Human-Computer Interaction, *34*(10), 913–921. doi:10.1080/10447318.2018.1471570

Joseph, J., & Mukesh, R. (2018). Detection of malware attacks on virtual machines for a self-heal approach in cloud computing using VM snapshots. *Journal of Communications Software and Systems*, *14*(3), 249-257. Retrieved from https://jcomss.fesb.unist.hr/index.php/jcomss

Joshi, C., & Singh, U. K. (2017). Information security risks management framework – A step towards mitigating security risks in university network. *Journal of Information Security and Applications*, 35, 128–137. doi: 10.1016/j.jisa.2017.06.006

Kallio, H., Pietila, A.-M., Johnson, M., & Kangasniemi, M. (2018). Systematic methodological review: developing a framework for a qualitative semistructured interview guide. *Journal Of Advanced Nursing*, *72*(12), 2954–2965. doi:10.1111/jan.13031

Karagiozis, N. (2018). The complexities of the researcher's role in qualitative research: The power of reflexivity. *International Journal of Interdisciplinary Educational Studies*, *13*(1), 19–31. doi:10.18848/2327-011X/CGP/v13i01/19-31

Kast, F. E., & Rosenzweig, J. E. (1972). General system theory: Applications for organization and management. *Academy of Management Journal*, *15*(4), 447. Retrieved from https://aom.org/research/journals/journal

Katz, D., & Kahn, R. L. (1969). *Common characteristics of open systems. Systems Thinking*. Harmondsworth, England: Penguin Books Ltd.

Kaur, G. (2016). Network security: Anti-virus. *International Journal of Advanced Research in Computer Science, 7*(6), 79-84. Retrieved from http://www.ijarcs.info/index.php/Ijarcs

Kaušpadienė, L., Ramanauskaitė, S., & Čenys, A. (2019). Information security management framework suitability estimation for small and medium enterprise. *Technological & Economic Development of Economy*, *25*(5), 979–997. doi:10.3846/tede.2019.10298

Kim, P., Homan, J. V., & Metzer, R. L. (2016). How long do employees remember information security training programs? A study of knowledge acquisition and retention. *Issues in Information Systems*, *17*(4), 197–207. Retrieved from https://www.iacis.org/iis/iis.php

Klein, S. (2017). Social systems: outline of a general theory. *Tempo Social*, *29*(3), 349–358. doi: 10.11606/0103-2070.ts.2017.125328

Kluge, A., Schüffler, A. S., Thim, C., Haase, J., & Gronau, N. (2019). Investigating unlearning and forgetting in organizations: Research methods, designs and implications. *The Learning Organization*, 26(5), 518–533. doi:10.1108/TLO-09-2018-0146

Koebel, J. T. (2017). Campus misconduct proceeding outcome notifications: A title Ix, Clery Act, and FERPA compliance blueprint. *Pace Law Review*, *37*(2), 551-588. Retrieved from https://www.digitalcommons.pace.edu/plr/vol37/iss2/4/

Koenigs, P. (2018). On the normative insignificance of neuroscience and dual-process theory. *Neuroethics*, *11*(2), 195–209. doi:10.1007/s12152-018-9362-y

Koohang, A., Anderson, J., Nord, J. H., & Paliszkiewicz, J. (2020). Building an awareness-centered information security policy compliance model. *Industrial Management & Data Systems*, *120*(1), 231–247. doi:10.1108/IMDS-07-2019-0412

Korstjens, I., & Moser, A. (2017a). Series: Practical guidance to qualitative research. Part 2: Context, research questions, and designs. *The European Journal of General Practice*, *23*(1), 274–279. doi:10.1080/13814788.2017.1375090

Korstjens, I., & Moser, A. (2017b). Series: Practical guidance to qualitative research. Part 4: Trustworthiness and publishing. *European Journal Of General Practice*, *24*(1), 120–124. doi:10.1080/13814788.2017.1375092

Kuchta, T., Palikareva, H., & Cadar, C. (2018). Shadow symbolic execution for testing software patches. *ACM Transactions on Software Engineering & Methodology*, *27*(3), 1–32. doi:10.1145/3208952

Kurniawan, A., & Riadi, I. (2018). Detection and analysis cerber ransomware based on network forensics behavior. *International Journal of Network Security*, *20*(5), 836-843. doi: 10.6633/IJNS.201809 20(5).04

Kvon, G. M., Vaks, V. B., Masalimova, A. R., Kryukova, N. I., Rod, Y. S., Shagieva, R. V., & Khudzhatov, M. B. (2018). Risk in implementing new electronic management systems at universities. *Eurasia Journal of Mathematics Science and Technology Education*, 14(3), 891–902. doi:10.12973/ejmste/81060

Kyegombe, N., Banks, M. L., Kelly, S., Kuper, H., & Devries, M. K. (2019). How to conduct good quality research on violence against children with disabilities: Key ethical, measurement, and research principles. *BMC Public Health, 19*(1), 1-14. doi:10.1186/s12889-019-7456-z

Lai, S. S., Pagh, J., & Zeng, F. H. (2019). Tracing communicative patterns: A comparative ethnography across platforms, media and contexts. *Nordicom Review*, *40*(1), 141–157. doi:/10.2478/nor-2019-0019

Lancaster, K. (2017). Confidentiality, anonymity and power relations in elite interviewing: conducting qualitative policy research in a politicized domain. *International Journal of Social Research Methodology, 20*(1), 93–103. doi:10.1080/13645579.2015.1123555

Le Blanc, A. M. (2017). Disruptive meaning-making: qualitative data analysis software and postmodern pastiche. *Qualitative Inquiry, 23*(*10)*, 789. Retrieved from https://journals.sagepub.com/home/qix

Lehmann, O. V., Murakami, K., & Klempe, S. H. (2019). Developmentally oriented thematic analysis (DOTA): A Qualitative research method to explore meaning-making processes in cultural psychology. *Forum: Qualitative Social Research*, *20*(2), 1–21. doi:10.17169/fqs-19.2.3190

Leukfeldt, E., Kleemans, E., & Stol, W. (2017). Origin, growth and criminal capabilities of cybercriminal networks. An international empirical analysis. *Crime, Law & Social Change*, *67*(1), 39–53. doi:10.1007/s10611-016-9663-1

Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *International Journal of Information Management*, *45*, 13–24. doi:10.1016/j.ijinfomgt.2018.10.017

Liao, H., & Hitchcock, J. (2018). Reported credibility techniques in higher education evaluation studies that use qualitative methods: A research synthesis. *Evaluation And Program Planning*, 68, 157–165. doi: 10.1016/j.evalprogplan.2018.03.005

Lim, I., Park, Y.-G., & Lee, J.-K. (2016). Design of security training system for individual users. *Wireless Personal Communications, 90*(3), 1105–1120. doi:10.1007/s11277-016-3380-z.

Lowe, A., Norris, A. C., Farris, A. J., & Babbage, D. R. (2017). Quantifying thematic saturation in qualitative data analysis. *Field Methods*, *30*(3), 191–207. doi:10.1177/1525822X17749386

Lowe, A., Norris, A. C., Farris, A. J., & Babbage, D. R. (2018). Quantifying thematic saturation in qualitative data analysis. *Field Methods*, *30*(3), 191–207. Retrieved from https://www.ebscohost-com/

Mabunda, S. (2019). Cyber extortion, ransomware and the South African cybercrimes and cybersecurity bill. *Statute Law Review*, 40(2), 143. Retrieved from https://journals.sagepub.com/loi/fmx

Mackieson, P., Shlonsky, A., & Connolly, M. (2019). Increasing rigor and reducing bias in qualitative research: A document analysis of parliamentary debates using applied thematic analysis. *Qualitative Social Work, 18*(6), 965–980. doi:10.1177/1473325018786996

Mahajan, L. S., Glew, L., Rieder, E., Ahmadia, G., Darling, E., Fox, E. H., … McKinnon,

M. (2019). Systems thinking for planning and evaluating conservation interventions. *Conservation Science and Practice, 1*(7). doi:10.1111/csp2.44

Maiorca, D., Demontis, A., Biggio, B., Roli, F., & Giacinto, G. (2020). Adversarial detection of flash malware: Limitations and open issues. *Computers & Security*, *96*(2020), 1-16. doi:10.1016/j.cose.2020.101901

Mania-Singer, J. (2017). A systems theory approach to the district central office's role in school-level improvement. *Administrative Issues Journal: Connecting Education, Practice, and Research*, *7*(1), 70–83. Retrieved from https://aij.scholasticahq.com/

Manion, R. F. (2016). Incentivizing the protection of personally identifying consumer data after the Home Depot breach. *Indiana Law Journal*, *91*(1), 143-164. Retrieved from http://ilj.law.indiana.edu/

Mansfield-Devine, S. (2016). Data protection: Prepare now or risk disaster. *Computer Fraud & Security*, *2016*(12), 5–12. doi:10.1016/S1361-3723(16)30098-7

Mansfield-Devine, S. (2018). Friendly fire: how penetration testing can reduce your risk. *Network Security, 2018*(6), 16–19. doi:10.1016/S1353-4858(18)30058-8

Mao, W., Cai, Z., Towsley, D., Feng, Q., & Guan, X. (2017). Security importance assessment for system objects and malware detection. *Computers & Security*, 68, 47–68. doi:10.1016/j.cose.2017.02.009

Marcus, D. J. (2018). The data breach dilemma: Proactive solutions for protecting consumers' Personal information. *Duke Law Journal*, *68*(3), 556–593. Retrieved from https://www.ebscohost.com/

Marek, M. W., & Skrabut, S. (2017). Privacy in educational use of social media in the U.S. *International Journal on E-Learning, 16*(3), 265–286. Retrieved from http://www.ejel.org/main.html

Martinelli, F., Marulli, F., & Mercaldo, F. (2017). Evaluating convolutional neural network for effective mobile malware detection. *Procedia Computer Science*, 112, 2372–2381. doi: 10.1016/j.procs.2017.08.216

Martinez-Mesa, J., Gonzalez-Chica, D. A., Duquia, R. P., Bonamigo, R. R., & Bastos, J. L. (2016). Sampling: How to select participants in my research study? *Anais Brasileiros De Dermatologia*, *91*(3), 326–330. doi:10.1590/abd1806-4841.20165254

McClain, E. K., Johnson-Moton, Y., Larsen, B., Ellis, R. J. B., & Niederhoffer, E. (2018). Making medicines: A case study in innovative academia-industry educational partnerships. *Industry and Higher Education*, *32*(5), 302–311. Retrieved from https://journals.sagepub.com/loi/ihe

Min, D., Park, D., Ahn, J., Walker, R., Lee, J., Park, S., & Kim, Y. (2018). Amoeba: An autonomous backup and recovery SSD for ransomware attack defense. *IEEE Computer Architecture Letters*, *17*(2), 243–246. doi:10.1109/LCA.2018.2883431

Misenheimer, K. J. (2016a). Faculty, staff, and student responsibilities for computer and information security on campus. *Journal of Information Systems Technology & Planning*, *8*(19), 1–11. Retrieved from http://www.intellectbase.org/

Misenheimer, K. J. (2016b). Training users to be aware of computer and information security on college and university campuses. *Journal of Information Systems*

Technology & Planning, *8*(19), 61. Retrieved from http://journalseek.net/cgi-bin/journal

Mohajan, K. H. (2018). Qualitative research methodology in social sciences and related subjects. *Journal of Economic Development, Environment and People*, *7*(1), 23-48. doi:10.26458/jedep.v7i1.571

Mohajan, K. H. (2017). Two criteria for good measurements in research: Validity and reliability. *Annals of Spiru Haret University Economic Series*, *17*(4), 59-82. doi:10.26458/1746

Mohurle, S., & Patil, M. (2017). A brief study of Wannacry threat: Ransomware attack. *International Journal of Advanced Research in Computer Science*, *8*(5), 1938-1940. Retrieved from http://www.ijarcs.info/index.php/Ijarcs

Moon, K., Brewer, T. D., Januchowski-Hartley, S. R., Adams, V. M., & Blackman, D. A. (2016). A guideline to improve qualitative social science publishing in ecology and conservation journals. *Ecology and Society*, *21*(3),17. doi:10.5751/ES-08663-210317

Mootz, J. J., Taylor, L., Wainberg, M. L., & Khoshnood, K. (2019). Ethical considerations for disseminating research findings on gender-based violence, armed conflict, and mental health: A case study from rural Uganda. *Health & Human Rights: An International Journal*, *21*(1), 81–92. Retrieved from https://www.hhrjournal.org/

Moreira, N., Molina, E., Lázaro, J., Jacob, E., & Astarloa, A. (2016). Cyber-security in substation automation systems. *Renewable and Sustainable Energy Reviews*, 54,1552-1562. doi: 10.1016/j.rser.2015.10.124

Moser, A., & Korstjens, I. (2018). Series: Practical guidance to qualitative research. Part 3: Sampling, data collection and analysis. *The European Journal of General Practice*, *24*(1), 9–18. doi:10.1080/13814788.2017.1375091

Motloch, L. J. (2017). Big history understanding of complexity, informatics and cybernetics. *Journal of Systemics, Cybernetics and Informatics*, *15*(6), 54-60. Retrieved from http://www.iiisci.org/journal/sci/home.asp

Mudiyanselage, A. K., & Pan, L. (2020). Security test moodle: a penetration testing case study. *International Journal of Computers & Applications*, *42*(4), 372–382. doi:10.1080/1206212X.2017.1396413

Münch, R. (1982). Talcott Parsons and the Theory of Action. II. The continuity of the development. *American Journal of Sociology*, *87*(4), 771–826. doi:10.1086/227522

Murshed, F., & Zhang, Y. (2016). Thinking orientation and preference for research methodology. *Journal of Consumer Marketing*, *33*(6), 437-446. doi:10.1108/JCM-01-2016-1694

Namanya, A. P., Awan, I. U., Disso, J. P., & Younas, M. (2019). Similarity hash-based scoring of portable executable files for efficient malware detection in IoT. *Future Generation Computer Systems*. doi: 10.1016/j.future.2019.04.044

National Center for Education Statistics. (2018). Data security dear colleague letter. Retrived from http://www.nces.ed.gov

National Commission for the Protection of Human Subjects of Biomedical and

Behavioral Research, B., MD. (1978). *The Belmont Report: Ethical Principles and Guidelines for the Protection of Human Subjects of Research.* Retrieved from https://www.hhs.gov/

Newton, V. L. (2017). "It's good to be able to talk": An exploration of the complexities of participant and researcher relationships when conducting sensitive research. *Women's Studies International Forum*, *61*(2017),93-99. doi: 10.1016/j.wsif.2016.11.011

O'Keeffe, J., Buytaert, W., Mijic, A., Brozović, N., & Sinha, R. (2016). The use of semi-structured interviews for the characterization of farmer irrigation practices. *Hydrology and Earth System Sciences*, *20*(5), 1911-1924. doi:10.5194/hess-20-1911-2016

O'Neil, M. (2014). Data breaches put a dent in colleges finances as well as reputations. *Chronicle of Higher Education*, *60*(27), A6–A8. Retrieved from https://www.chronicle.com/

Ochieng, N., Mwangi, W., & Ateya, I. (2019). Optimizing computer worm detection using ensembles. *Security and Communication Networks*, 1-10. doi:/10.1155/2019/4656480

Ogarkova, A., Soriano, C., & Gladkova, A. (2016). Methodological triangulation in the study of emotion. *Review of Cognitive Linguistics*, *14*(1), 73–101. doi: 10.1075/rcl.14.1.04oga

Ohi, F. (2017). From a binary-state system to a multi-state system. *International Journal of Industrial Engineering*, *24*(4), 340–365. Retrieved from http://ijiemjournal.uns.ac.rs/

Okyere, S. (2018). “Like the stranger at a funeral who cries more than the bereaved”: Ethical dilemmas in ethnographic research with children. *Qualitative Research, 18*(6), 623–637. doi:10.1177/1468794117743464

Olukoya, O., Mackenzie, L., & Omoronyia, I. (2020). Towards using unstructured user input request for malware detection. *Computers & Security, 93*(2020),1-18. doi:10.1016/j.cose.2020.101783

Onwuegbuzie, A. J., & Collins, K. M. T. (2017). The role of sampling in mixed methods-research enhancing inference quality. *Kolner Zeitschrift fur Soziologie und Sozialpsychologie, 69,* 133–156. doi:10.1007/s11577-017-0455-0

Osborne, C. L. (2016). The legal research plan and the research log: An examination of the role of the research plan and research log in the research process. *Legal Reference Services Quarterly, 35*(3), 179–194. doi:10.1080/0270319X.2016.1227205

Palega, M., & Knapinski, M. (2018). Threats associated with the human factor in the aspect of information security. *Scientific Journal of the Military University of Land Forces, 187*(1), 105–118. doi:10.5604/01.3001.0011.7364

Paliszkiewicz, J. (2019). Information security policy compliance: Leadership and trust. *Journal of Computer Information Systems, 59*(3), 211–217. doi:10.1080/08874417.2019.1571459

Pangeni, S. K. (2017). Issues in E-Research: Log in/out virtual fields. *Turkish Online Journal of Distance Education,* 18(3). Retrieved from https://teachonline.ca/fr/node/89558

Pathari, V., & Sonar, R. (2012). Identifying linkages between statements in information security policy, procedures and controls. *Information Management & Computer Security*, *20*(4), 264–280. doi:10.1108/09685221211267648

Patil, S., Jangra, A., Bhale, M., Raina, A., & Kulkarni, P. (2017). Ethical hacking: The need for cyber security. *2017 IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI), Power, Control, Signals and Instrumentation Engineering (ICPCSI), 2017 IEEE International Conference On*, 1602–1606. doi:10.1109/ICPCSI.2017.8391982

Patton, M. (2015). Battling data breaches: For higher education institutions, data breach prevention is more complex than for industry and business. *Community College Journal*, *86*(1), 20–24. Retrieved from http://www.ebscohost.com/

Pérez-González, D., Preciado, T. S., & Solana-Gonzalez, P. (2019). Organizational practices as antecedents of the information security management performance : An empirical investigation. *Information Technology & People*, *32*(5), 1262–1275. doi:10.1108/ITP-06-2018-0261

Pieters, W. W. (2017). Beyond individual-centric privacy: Information technology in social systems. *Information Society*, *33*(5), 271–281. doi:10.1080/01972243.2017.1354108

Porvazník, J., & Ljudvigová, I. (2016). General theory of systems, cybernetics, and evaluation of human competence by solving present crisis problems of civilization. *Procedia - Social and Behavioral Sciences*, *230*, 112–120. doi:

10.1016/j.sbspro.2016.09.014

Prada-Ramallal, G., Roque, F., Herdeiro, M. T., Takkouche, B., & Figueiras, A. (2018). Primary versus secondary source of data in observational studies and heterogeneity in meta-analyses of drug effects: A survey of major medical journals. *Bmc Medical Research Methodology*, *18*(1), 1-14. doi:10.1186/s12874-018-0561-3

Rahi, S. (2017). Research design and methods: A systematic review of research paradigms, sampling issues and instruments development. *International Journal of Economics & Management Sciences,6*(2), 1-5. doi: 10.4172/2162-6359.1000403

Rahman, M. S. (2017). The advantages and disadvantages of using qualitative and quantitative approaches and methods in language "testing and assessment" research: A literature review. *Journal of Education and Learning*, *6*(1), 102–112. Retrieved from http://www.ccsenet.org/journal/index.php/jel

Rajab, M., & Eydgahi, A. (2019). Evaluating the explanatory power of theoretical frameworks on intention to comply with information security policies in higher education. *Computers & Security*, 80, 211–223. doi: 10.1016/j.cose.2018.09.016

Reid, R., & Niekerk, V. J. (2016). Decoding audience interpretations of awareness campaign messages. *Information & Computer Security*, *24*(2), 177–193. doi:10.1108/ICS-01-2016-0003.

Reilly, T. M., & Jones, I. R. (2017). Mixed methodology in family business research: Past accomplishments and perspectives for the future. *Journal of Family Business*

Strategy, *8*(3), 185–195. doi:10.1016/j.jfbs.2017.08.003

Renbarger, R. L., Sulak, T. N., & Kaul, C. R. (2019). Finding, accessing, and using secondary data for research on gifted education and advanced academics. *Journal of Advanced Academics*, *30*(4), 463–473. doi:10.1177/1932202X19864117

Rhiannon, E., & Hurrell, C. (2016). The role of schools in children and young people's self-harm and suicide: Systematic review and meta-ethnography of qualitative research. *BMC Public Health*, *16*(1), 1-16. doi:10.1186/s12889-016-3065-2

Richard, V., & Bélanger, M. (2018). Accepting research: Teachers' representations of participation in educational research projects. *International Journal of Educational Methodology*, *4*(2), 61–73. Retrieved from https://www.ijem.com/

Richards, S. (2018). Research design in social work: Qualitative and quantitative methods. *Journal of Social Work*, *18*(6), 755–756. doi:10.1177/1468017318787592

Richardson, R., & North, M. (2017). Ransomware: Evolution, mitigation and prevention. *International Management Review*, *13*(1), 10–21. Retrieved from http://www.imrjournal.org/

Rinehart, E. K. (2019). Researchers as poets: Anonymity and fidelity in crafting participant "portraits." *Qualitative Inquiry*, *25*(9/10), 862–865. doi:10.1177/1077800418787555

Roberts, K., Dowell, A., & Nie, J. (2019). Attempting rigour and replicability in thematic analysis of qualitative research data; a case study of codebook development. *BMC Medical Research Methodology*, *19*(1), 1-8. doi:10.1186/s12874-019-0707-y

Roller, M. R., & Lavrakas, P. J. (2018). A total quality framework approach to sharing qualitative research data: comment on Dubois et al. *Qualitative Psychology*, *5*(3), 394-401. doi:10.1037/qup0000134

Rothgangel, M., & Saup, J. (2017). Classroom research in religious education: The potential of grounded theory. *HTS Teologiese Studies/Theological Studies*, *73*(4), e1-e10. doi:10.4102/hts.v73i4.4638

Rrushi, J. L. (2016). NIC displays to thwart malware attacks mounted from within the OS. *Computers & Security*, 61, 59–71. doi: 10.1016/j.cose.2016.05.002

Saheb, M. H. (2013). University information security policy: Case study. (English). *Cybrarians Journal*, *33*, 1–14. Retrieved from http://www.journal.cybrarians.info/

Sahin, C. (2018). Social media addiction scale-student form: The reliability and validity study. *Turkish Online Journal of Educational Technology - TOJET*, *17*(1), 169–182. Retrieved from http://www.tojet.net/

Sarikaa, S., & Paul, V. (2017). Parallel phishing attack recognition using software agents. *Journal of Intelligent & Fuzzy Systems*, *32*(5), 3273–3284. doi:10.3233/JIFS-169270

Saunders, B., Sim, J., Kingstone, T., Baker, S., Waterfield, J., Bartlam, B., … Jinks, C. (2018). Saturation in qualitative research: Exploring its conceptualization and operationalization. *Quality & Quantity*, *52*(4), 1893–1907. doi:10.1007/s11135-017-0574-8.

Schadler, C. (2019). Enactments of a new materialist ethnography: Methodological framework and research processes. *Qualitative Research*, *19*(2), 215–230. doi:10.1177/1468794117748877

Scharp, K. M., & Sanders, M. L. (2019). What is a theme? Teaching thematic analysis in qualitative communication research methods. *Communication Teacher, 33*(2), 117–121. Retrieved from https://www.tandfonline.com/loi/rcmt20

Schelbe, L., Randolph, K. A., Yelick, A., Cheatham, L. P., & Groton, D. B. (2018). Systems theory as a framework for examining a college campus-based support program for the former foster youth. *Journal of Evidence-Informed Social Work*, *15*(3), 277–295. doi:10.1080/23761407.2018.1436110

Sen, R., & Borle, S. (2015). Estimating the contextual risk of data breach: An empirical approach. *Journal of Management Information Systems*, *32*(2), 314–341. doi:10.1080/07421222.2015.1063315

Shah, B. (2017). Cisco umbrella: A cloud-based secure internet gateway (SIG) on and off network. *International Journal of Advanced Research in Computer Science*, *8*(2), 4-7. Retrieved from http://www.ijarcs.info/index.php/Ijarcs

Shapka, J. D., Domene, J. F., Khan, S., & Yang, L. M. (2016). Online versus in-person interviews with adolescents: An exploration of data equivalence. *Computers in Human Behavior*, *58*, 361–367. doi: 10.1016/j.chb.2016.01.016

Sharma, A., Gandotra, E., Bansal, D., & Gupta, D. (2019). Malware capability assessment using fuzzy logic. *Cybernetics & Systems*, *50*(4), 323–338. doi:10.1080/01969722.2018.1552906

Shawver, Z., Griffith, J. D., Adams, L. T., Evans, J. V., Benchoff, B., & Sargent, R.

(2016). An examination of the WHOQOL-BREF using four popular data collection methods. *Computers in Human Behavior, 55*(Part A), 446–454. doi: 10.1016/j.chb.2015.09.030.

Shen, J., Gao, X., & Xia, J. (2017). School as a loosely coupled organization? An empirical examination using national SASS 2003-04 Data. *Educational Management Administration & Leadership*, *45*(4), 657–681. Retrieved from https://journals.sagepub.com/

Sim, J., Saunders, B., Waterfield, J., & Kingstone, T. (2018). The sample size debate: Response to Norman Blaikie. *International Journal of Social Research Methodology*, *21*(5), 643–646. Retrieved from https://www.tandfonline.com/toc/tsrm20/current

Smith, T., & Smith, S. (2018). Reliability and validity of the research methods skills assessment. *International Journal of Teaching and Learning in Higher Education*, *30*(1), 80–90. Retrieved from http://www.isetl.org/ijtlhe/

Smyth, G. (2017). Using data virtualisation to detect an insider breach. *Computer Fraud & Security, 2017*(8), 5–7. doi:10.1016/S1361-3723(17)30068-4

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

Sowmya, P., & Chatterjee, M. (2018). Comparative study of threats and solutions in online social networks. *International Journal of Advanced Research in Computer Science, 9*(1), 760-764. Retrieved from http://www.ijarcs.info/index.php/Ijarcs

Spekle, R. F., & Widener, S. K. (2018). Challenging issues in survey research: Discussion and suggestions. *Journal of Management Accounting Research, 30*(2), 3-21. Retrieved from https://aaahq.org/MAS/JMAR

Spiers, J., Morse, M. J., Olson, K., Mayan, M., & Barrett, M. (2018). Reflection/commentary on a past article: “Verification strategies for establishing reliability and validity in qualitative research.” *International Journal of Qualitative Methods*. doi:10.1177/1609406918788237

Surmiak, A. (2018). Confidentiality in qualitative research involving vulnerable participants: researchers’ perspectives. *Forum: Qualitative Social Research*, *19*(3), 393–418. doi:10.17169/fqs-19.3.3099

Tan, X., & Yu, F. (2018). Research and application of virtual user context information security strategy based on group intelligent computing. C*ognitive Systems Research*. *52*,629-639. doi: 10.1016/j.cogsys.2018.08.016.

Teece, D. J. (2018). Dynamic capabilities as (workable) management systems theory. J*ournal of Management & Organization*, *24*(3), 359–368. doi:10.1017/jmo.2017.75

Thomas, D. R. (2017). Feedback from research participants: Are member checks useful in qualitative research? *Qualitative Research In Psychology*, *14*(1), 23–41. doi:10.1080/14780887.2016.1219435

Thomas, G., Burmeister, O., & Low, G. (2019). The importance of ethical conduct by penetration testers in the age of breach disclosure laws. *Australasian Journal of Information Systems*, *23*(0). doi:10.3127/ajis.v23i0.1867

Thompson, R. (2018). A qualitative phenomenological study of emotional and cultural intelligence of international students in the United States of America. *Journal of International Students*, *8*(2), 1220-1255. doi:10.5281/zenodo.1250423

Tobi, H., & Kampen, J. K. (2018). Research design: The methodology for interdisciplinary research framework. *Quality & Quantity,52*(3), 1209-1225. doi.org/10.1007/s11135-017-0513-8

Touchette, F. (2016). The evolution of malware. *Network Security*, *2016*(1), 11–14. doi:10.1016/S1353-4858(16)30008-3

Tran, V.-T., Porcher, R., Falissard, B., & Ravaud, P. (2016). Point of data saturation was assessed using resampling methods in a survey with open-ended questions. *Journal of Clinical Epidemiology*, *80*, 88–96. doi: 10.1016/j.jclinepi.2016.07.014

Tran, V.-T., Porcher, R., Tran, V.-C., & Ravaud, P. (2017). Predicting data saturation in qualitative surveys with mathematical models from ecological research. *Journal of Clinical Epidemiology*, *82*, 71–78. doi: 10.1016/j.jclinepi.2016.10.001

Valiente, J. C. (2017). Addressing malware with cybersecurity awareness. *ISSA Journal*, *15*(10), 16–22. Retrieved from http://www.doaj.org/

Van Assche, K., Valentinov, V., & Verschraegen, G. (2019). Ludwig von Bertalanffy and his enduring relevance: Celebrating 50 years general system theory. *Systems Research & Behavioral Science*, *36*(3), 251–254. doi:10.1002/sres.2589

Varpio, L., Ajjawi, R., Monrouxe, L. V., O'Brien, B. C., & Rees, C. E. (2017). Shedding the cobra effect: problematising thematic emergence, triangulation, saturation and member checking. *Medical Education, 51*(1), 40–50. doi:10.1111/medu.13124

Varsos, D. S., Giannakou, A. S., & Assimakopoulos, A. N. (2019). A systems approach to information security for the twenty-first century organization. *Journal of the European Union for Systemics*, 9. doi: https://doi.org/10.14428/aes.v9i1

Vasileiou, K., Barnett, J., Thorpe, S., & Young, T. (2018). Characterising and justifying sample size sufficiency in interview-based studies: Systematic analysis of qualitative health research over a 15-year period. *BMC Medical Research Methodology*, *18*(1),1-18. doi:10.1186/s12874-018-0594-7

Velte, P., & Stawinoga, M. (2017). Integrated reporting: The current state of empirical research, limitations and future research implications. *Journal of Management Control, 28*(3), 275-320. doi: 10.1007/s00187-016-0235-4

Venter, I. M., Blignaut, R. J., Renaud, K., & Venter, M. A. (2019). Cyber security education is as essential as “the three R’s.” *Heliyon*, *5*(12). doi:10.1016/j.heliyon.2019.e02855

Vila-Henninger, L. A. (2019). Turning talk into “rationales”: Using the extended case method for the coding and analysis of semistructured interview data in ATLAS.ti. *Bulletin de Methodologie Sociologique*,*143*(1), 28–52. doi:10.1177/0759106319852887

von Bertalanffy, L. (1951). Theoretical models in biology and psychology. *Journal of Personality*, *20*(1), 24. doi:10.1111/j.1467-6494. 1951.tb01511.x von Bertalanffy, L. (1968). *General systems theory: Foundations, development, application* (Rev. ed.). New York, NY: George Braziller.

Wallingford, J., Peshwa, M., & Kelly, D. (2019). Towards understanding the value of ethical hacking. *Proceedings of the International Conference on Cyber Warfare & Security*, 639–649. Retrieved from https://www.academic-conferences.org/conferences/iccws/

Wang, S., Wang, P., & Zhang, Y. (2020). A prediction method for urban heat supply based on grey system theory. *Sustainable Cities and Society*, 52. doi:10.1016/j.scs.2019.101819

Wei, H., Mao, B., Oberg, J., & Kastner, R. (2016). Detecting hardware trojans with gate-level information-flow tracking. *Computer*, *49*(8), 44-55. doi:10.1109/MC.2016.225

Weil, S. (2017). The advantages of qualitative research into femicide. *Przeglad Socjologii Jakosciowej*, *13*(3), 118–125. Retrieved from http://www.qualitativesociologyreview.org/PL/index_pl.php

Weishäupl, 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. doi: 10.1016/j.cose.2018.02.001

Werder, K., & Maedche, A. (2018). Explaining the emergence of team agility: A complex adaptive systems perspective. *Information Technology & People*, *31*(3), 819–844. doi:10.1108/ITP-04-2017-0125

Whitson, R. (2017). Digital contagions: A media archaeology of computer viruses, 2nd edition. *Theory Culture & Society*, *34*(7–8), 293–298. doi:10.1177/0263276417736593

Wijaya, D. H., Gunawan, W., Avrizal, R., & Arif, M. S. (2020). Designing chatbot for college information management. *IJISCS (International Journal of Information System and Computer Science)*, *4*(1), 8–13. Retrieved from http://www.doaj.org/

Wine, O., Ambrose, S., Campbell, S., Villeneuve, P. J., Burns, K. K., & Vargas, A. O. (2017). Key components of collaborative research in the context of environmental health: A scoping review. *Journal of Research Practice*, 13(2), 1-13. Retrieved from http://jrp.icaap.org/index.php/jrp

Woltjer, R. (2017). Workarounds and trade-offs in information security – an exploratory study. *Information & Computer Security*, *25*(4), 402–420. doi:10.1108/ICS-02-2016-0017

Xiaobo, M., Ying, C., & Jinhua, G. (2019). Analysis of computer network information security and protection strategy. *MATEC Web of Conferences*, 02013. doi:10.1051/matecconf/201926702013

Yevdokymenko, M., Mohamed, E., & Onwuakpa, P. (2017). Ethical hacking and penetration testing using raspberry PI. *2017 4th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T), Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T), 2017 4th International*, 179–181. doi: 10.1109/INFOCOMMST.2017.8246375

Yilmaz, R., & Yalman, Y. (2016). A comparative analysis of university information systems within the scope of the information security risks. *TEM Journal*, *5*(2), 180–191. doi:10.18421/TEM52-10

Zahle, J. (2018). Data, epistemic values, and multiple methods in case study research. *Studies in History and Philosophy of Science*, *78,*32-39. doi: 10.1016/j.shpsa.2018.11.005

Zakarya, A. A. (2018). Information security practice in Saudi Arabia: case study on Saudi organizations. *Information & Computer Security*, *26*(5), 568–583. doi:10.1108/ICS-01-2018-0006

Zeadally, S., Isaac, J. T., & Baig, Z. (2016). Security attacks and solutions in electronic health (E-health) systems. *Journal of Medical Systems*, *40*(12), 1-12. doi:10.1007/s10916-016-0597-z

Zeinab, A. (2019). A practical road map for assessing cyber risk. *Journal of Risk Research*, *22*(1), 32–43. doi:10.1080/13669877.2017.1351467.

Zhong, W., & Gu, F. (2019). A multi-level deep learning system for malware detection. *Expert Systems with Applications*, *133*, 151–162. doi: 10.1016/j.eswa.2019.04.064

Appendix A: Email Invitation to Chief Information Officers

Dear <CIOs name>,

I am Felix Agyei, a Doctor of Information Technology student at Walden University. I am conducting interviews as part of a research study to ascertain the strategies information technology leaders in universities and colleges use to prevent malware attacks. My study is approved by Walden University's Institutional Review Board.

I am asking your permission to contact leaders in your IT staff who are knowledgable about the adoption of strategies to prevent information security breaches. I propose to contact each individual by email to explain the process and to set up a time for an interview. The participant will sign an informed consent form prior to the interview. The approximate length of the interview is between 30 to 60 minutes and all gathered information will be confidential through the utilization of pseudonyms and coding. The disclosure of personally identifiable information will be avoided.

There is no direct compensation for participation. However, your involvement could contribute valuable information to the information technology field in terms of malware prevention strategies. I will provide you with a report of my findings, which includes strategies used by other California universities after my project has been accepted for publication.

In case you are willing for your organization to be involved in this study, please indicate your authorization by email and please provide me with names, titles, and email addresses of at least three IT leaders in your organization who have expertise in the adoption of strategies to prevent information security breaches.

If you have any questions, please don’t hesitate to ask.

Thank you,

Felix Agyei

Doctor of InformationTechnology student

Walden University

Appendix B: Research Participation Invitation Letter

Dear <participant name>,

I am Felix Agyei, a Doctor of Information Technology student at Walden University. I am conducting interviews as part of a research study to ascertain the strategies information technology leaders in universities and colleges use to prevent malware attacks. My study is approved by Walden University's Instituational Review Board. Your CIO, <name>, has given me permission to contact you.

As a technical leader, you are in an ideal position to provide valuable information from your experience and perspective. This will be an informal interview lasting between 30 and 60 minutes. The objective is to try and capture your experiences and perspectives about the mitigation and prevention strategies for malware attacks in universities and colleges. Your responses to the interview questions will be kept confidential. The interview will be assigned codes and pseudonyms to prevent the disclosure of personal identifiers during the data analysis and findings. I will follow up the interview with an email asking you to confirm my understanding of your comments. That confirmation process should only take about 10 minutes. I will also ask you to provide copies of your organization’s documentation that addresses strategies you use to prevent malware attacks.

There is no compensation for participating in this research exercise. However, your participation will serve as a valuable input to the study findings and could contribute to existing knowledge about malware prevention strategies to the public and IT practitioners.

If you agree to participate, please sign the attached informed consent form and return it to me by email. Please also suggest a suitable day, time, and medium of the interview (i.e. phone, video call or in-person).

Please do not hesitate to ask any questions.

Thank you,

Felix Agyei

Doctor of Information Technology student

Walden University

Appendix C: Interview Protocol

Interview: Strategies to Prevent Malware Attacks in Universities and Colleges

Participant ID:____________________Date:_______________Starting Time:____________

A. The interview will commence with an overview of the research topic.

B. I will show my appreciation to each study subject for honoring the invitation to participate in the research.

C. Study subjects will be reminded the interview is being recorded and that all gathered information will be absolutely confidential.

D. After briefing the study subjects about the confidentiality of the collected data, I will start recording.

E. Each interview session will last around 30 to 40 minutes or until all questions have been answered.

F. Before the concluding sections of the interview, study participants will be asked to provide any organizational documents to support interview responses.

G. The concluding session of the interview will be focused on an explanation of the concept of member checking.

H. The interview session will end with a thank you for participation, once all question responses have been confirmed to the satisfaction of study subjects.

Interview Follow-Up

Script: I like to express my appreciation for an opportunity for a 10-minute follow-up email to review my interpretation and to also offer you the chance to rectify any errors or contribute additional information deemed fit.

Interview Question	**Did my interpretation correctly reflect your intended response? Or is there any additional information you'll like to contribute?**
Do you personally have training in malware attacks? If not, why not? If so, how effective has the training be?	**Interpretation:**
	Comments:
What strategies have been employed to protect the institution's information systems from malware attacks?	**Interpretation:**
	Comments:
What strategies failed to protect the institution's information systems from malware attacks?	**Interpretation:**
	Comments:
Are there both internal and external attacks in this institution? If so which are most destructive?	**Interpretation:**
	Comments:
Does this organization provide an adequate budget to address malware attacks?	**Interpretation:**
	Comments:
Are staff equipped with the needed skills to address malware attacks?	**Interpretation:**
	Comments:
What are the biggest sources of malware attacks in this institution?	**Interpretation:**
	Comments:
What policies have you adopted in relation to dealing with malware sources in this institution?	**Interpretation:**
	Comments:
What additional information do you want to share in regard to strategies to prevent malware attacks in the university's or college's information systems?	**Interpretation:**
	Comments:

Appendix D: Interview Questions

- Do you personally have training in malware attacks? If not, why not? If so, how effective has the training been?
- What strategies have been employed to protect the institution’s information systems from malware attacks?
- What strategies failed to protect the institution’s information systems from malware attacks?
- Are there both internal and external attacks in this institution? If so which are most destructive?
- Does this organization provide an adequate budget to address malware attacks?
- Are staff equipped with the needed skills to address malware attacks in this institution?
- What are the biggest sources of malware in this institution?
- What policies have you adopted in relation to dealing with malware attacks in this institution?
- What additional information do you want to share in regard to strategies to prevent malware attacks in the university’s or college’s information systems?