2021

Strategies Security Managers Used to Prevent Security Breaches in SCADA Systems' Networks

Oladipo Ogunmesa
Walden University

Walden University

College of Management and Technology

This is to certify that the doctoral study by

Oladipo Ogunmesa

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. Bob Duhainy, Committee Chairperson, Information Technology Faculty
Dr. Donald Carpenter, Committee Member, Information Technology Faculty
Dr. Jodine Burchell, University Reviewer, Information Technology Faculty

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

Walden University
2021

Abstract

Strategies Security Managers Used to Prevent Security Breaches in SCADA Systems' Networks

by

Oladipo Ogunmesa

MS. Walden University, 2019

MA, Webster University, 2013

BS, Ondo State University, 1996

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Information Technology

Walden University

August 2021

Abstract

Supervisory Control and Data Acquisition (SCADA) systems monitor and control physical processes in critical infrastructure. The impact of successful attacks on the SCADA systems includes the system's downtime and delay in production, which may have a debilitating effect on the national economy and create critical human safety hazards. Grounded in the general systems theory, the purpose of this qualitative multiple case study was to explore strategies SCADA security managers in the Southwest region of the United States use to secure SCADA systems' networks. The participants comprised six SCADA security managers from three oil and gas organizations in the midstream sector located within this region. Data were collected using semistructured interviews and a review of organizational documents. Four themes emerged from the thematic analysis: (a) the importance of security awareness and workforce security training, (b) the use of technical control mechanisms, (c) the establishment of standard security policies, and (d) the use of access and identity management techniques. A key recommendation is for IT managers to adopt security awareness and workforce security training to strengthen the security chain's most vulnerable link. The implications for positive social change include the potential to prevent consequences such as loss of lives, damage to the environment, and the economy resulting from malicious activities.

Strategies Security Managers Used to Prevent Security Breaches in SCADA Systems' Networks

by

Oladipo Ogunmesa

MS, Walden University, 2019

MA, Webster University, 2013

BS, Ondo State University, 1996

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Information Technology

Walden University

August 2021

Dedication

I dedicate this work to my wife, Oluwabusayo, and our beautiful daughters, Oluwatise, Oluwanifemi, Oluwafetemi, and Oluwadara. Thank you for your support and understanding. Without all of you, I would not have been able to complete this work.

Acknowledgments

First of all, I wish to thank God for granting me the grace to start and finish my doctoral study. I want to appreciate Dr. Bob Duhainy, my committee chair, that guided me throughout the process and ensured my success. Your mentoring kept me focused and ensured I remained centered. I say thank you. To my second committee member Dr. Don Carpenter, I am grateful for your prompt feedback, suggestions, and thoughts as the study developed. To my URR, Dr. Jodine Burchell, I am thankful for the thorough work of scrutinizing my work and your support throughout the process. Thanks for your recommendations and your feedback.

I wish to thank my sister and her husband, Pastor (Dr.) Ayobami, and Pastor (Mrs.) Omodele Awe for bringing me into this country and their support during this doctoral study. I cannot but appreciate my parents Chief & Chief (Mrs.) E. Olu Ogunmesa for the discipline instilled in me and for teaching me the benefits of hard work. Lastly, I am grateful to every family member for your inspiration, support, and encouragement during my doctoral research. To all my friends, I am so thankful for your help.

Table of Contents

List of Tables

Section 1: Foundation of the Study

This study focused on exploring supervisory control and data acquisition (SCADA) security managers' strategies to secure the systems' networks to prevent security breaches using a qualitative multiple case study. The SCADA systems monitor and control critical infrastructures crucial to modern life, such as water pumps and electricity grids (Rakas et al., 2020). According to Shlomo et al. (2021), more reports concerning cyberattacks on the systems have surfaced in the media, such as the Stuxnet worm, a famous attack. Attacks on the SCADA system may result in loss of lives, economic losses, financial losses, and environmental destruction (Stănculescu et al., 2021). This study's findings would benefit security managers by increasing their understanding and knowledge of cyberattacks and their strategies to secure and protect the SCADA systems.

Background of the Problem

In this research study, I explored the security challenges experienced by the SCADA systems. Organizations use SCADA systems to control critical infrastructures crucial to modern life, such as water pumps, electricity grids, and oil and gas midstream pipelines (Kalech, 2019). The awareness and the critical importance of the system were initially limited. SCADA systems were secure in the past because they used isolated networks and proprietary protocols (Upadhyay & Sampalli, 2020). Financial needs and performance requirements necessitate the need to connect the SCADA system to the internet over the last 2 decades, according to Kalech (2019). The system is at high risk of being attacked by highly skilled cyber attackers because of the increased interconnected devices which exposed its vulnerabilities. According to Upadhyay and Sampalli (2020), standard software and hardware components make the SCADA system the target of traditional security vulnerabilities and attack methods.

Securing the SCADA system is of utmost significance because a cyber-physical attack of the system can disrupt the physical process, resulting in severe economic consequences, equipment damage, safety, or security ramifications (Nazir et al., 2017). The security concerns of the system were initially limited to physical attacks because only authorized personnel can assess the system. The integration of the modern-day SCADA systems within the global internet, local intranet, and corporate networks caused the many security problems faced by the system. Cyber attackers explore the vulnerabilities within the system, and the breaches are caused by security that was lacking within the organizations' SCADA systems.

Problem Statement

The SCADA system has become the target of cyberattacks due to its sensitive operations (Li et al., 2016). In 2015, the BlackEnergy attack was launched against the SCADA system, which caused an outage for power distribution of 27 substations and led to the loss of power for about 225,000 customers (Clark et al., 2017). The general IT problem is that oil and gas organizations in the midstream sector suffer data breaches due to security threats to SCADA systems. The specific IT problem is that some SCADA security managers lack strategies to secure SCADA systems' networks to prevent security breaches.

Purpose Statement

The purpose of this qualitative multiple case study was to examine the strategies used by SCADA systems' security managers to secure SCADA systems' networks to prevent security breaches. The target population consisted of SCADA security managers who have strategies to secure SCADA systems' networks. The SCADA security managers required for this study were selected from oil and gas organizations in the midstream sector in the Southwest region of the United States. The implication for positive social change may include discouraging attackers with malicious intent from triggering a breakdown in critical infrastructures that keep the society functioning, such as electrical systems, oil and gas pipelines, and water distribution systems.

Nature of the Study

Qualitative methodology was the approach used for this study based on understanding and reviewing the available research methods. A deeper understanding of what is yielded from a process can be uncovered by researchers that used a qualitative approach (Bansal et al., 2018). Since the focus of this study was to explore in-depth the strategies used by SCADA security managers to secure SCADA systems' networks, I used the qualitative method to determine the strategy that worked, the ones that did not work, and why. Researchers use a quantitative research method when the intention is to test a hypothesis from the obtained data (Scrutton & Beames, 2015). A quantitative approach was not appropriate for this study because my intention was not to test a hypothesis. According to Syrjä et al. (2019), a mixed-method approach may be used when the purpose of the study requires synthesizing ideas from both qualitative and quantitative methods. Since I have already ruled out quantitative methods, I did not select the mixed-method approach for this study.

I used a multiple case study design for this study. According to Jarvis and Williams (2017), case studies are appropriate in qualitative research when exploring complex issues through one or more sources. I chose a multiple case study design to explore complex issues such as the strategies used by the SCADA security managers to secure SCADA systems' networks in their real-life settings. The use of multiple case study is especially true when it involves data collection from different sources to depict and analyze complex issues, which is the main idea behind this study. Therefore, an appropriate design used for this study was the multiple case study. Other design options that I considered for this study were ethnographic and phenomenological. The ethnographic design focuses on the society or culture under review, often prompting a vital firm relationship between the ethnographers and participants (Kaley et al., 2019). I did not use the ethnographic design because this study did not focus on culture. The phenomenological approach uses the participants' lived experiences and subjective viewpoints to interpret a particular phenomenon's human experience (Alfakhri et al., 2018). A phenomenological design was not chosen for my study because the study did not focus on the human lived experience.

Research Question

What strategies do SCADA security managers use to secure SCADA systems' networks to prevent security breaches?

Interview Questions

1. What influenced the development of SCADA systems' security in your organization?
2. Can you tell me about the tools and techniques used in securing the SCADA systems?
3. How useful are these tools and techniques?
4. How effective and efficient are the methods used in preventing data breaches on SCADA systems' networks?
5. What methods are ineffective in preventing data breaches on SCADA systems' networks?
6. What challenges did you face while executing and implementing these methods?
7. In your experience, which of these methods, technical, formal, or informal, have you found the most effective?
8. What impact do technical, formal, and informal strategies have on one another from your experience?
9. In your experience, what are the determining factors on how to implement SCADA security, compliance practices, and cybersecurity training?
10. What can be done to prevent internal attacks by insiders on SCADA systems' networks?

Conceptual Framework

This study's conceptual framework was driven by the general systems theory (GST). The scholar Bertalanffy (1972) first proposed GST in 1946. Enhanced systems thinking and the combination of different natural and artificial systems focus on GST (Malecic, 2017). GST is the study of wholes and wholeness, and according to Phipps (2019), the phenomenon should be observed as a whole and not as a separate part. The organization system consists of structure, leadership, high-performance work practice, and highly interdependent strategy (Hartnell et al., 2019). All the interdependent elements within an organization must function well to accomplish the objectives of the organization. One of the critical elements of an organization is information security, which may be crucial to its long-term success (Abraham & Nair, 2018). According to Mar (2019), a failure of part of a system may prevent the entire system from working. Therefore, GST was used to show how the information security strategies that I presented in this study will help bring about the accomplishments of organizational objectives.

Researchers use GST to understand the completeness of organizations when all subsystems within a system collaborate to ensure the accomplishment of its goals (Simola, 2018). One of the critical business parts of an organization is information security (Abraham & Nair, 2018). However, security threats are one of the biggest challenges affecting the organization networks, inducing a security defense breakdown that intensifies the in-depth defense mechanism of the system (Ahanger & Aljumah, 2019). GST applied to this study because it provided a framework to examine what strategies SCADA security managers used to secure the SCADA systems' network, thereby accomplishing the organization's goals.

Operational Definitions

Critical infrastructure: Vital assets such as water supply, power generation and supply, manufacturing facilities, and transportation networks of national importance (Nazir et al., 2017).

Human machine interface (HMI): HMI displays the current state information of physical processes within the SCADA systems (Chekole et al., 2020).

Industrial Control System (ICS): ICS is usually found in the industrial sectors, and they include SCADA systems, programmable logic controllers (PLC), and distributed control systems (Bhamare et al., 2020).

Information security manager: Security managers are responsible for identifying and prioritizing security threats, and for allocating the limited protection measures efficiently (Arghavani et al., 2018).

Programmable logic controller (PLC): PLCs are industrial-grade digital computers used for performing control functions in industrial applications (Kalech, 2019).

Remote telemetry unit (RTU): RTU directly controls field devices such as actuators, sensors, and motors that perform specific operations (Li et al., 2019).

SCADA system: Supervisory Control and Data Acquisition system is used for monitoring and controlling physical processes in critical infrastructures such as water plants, oil and gas pipelines, power plants, and smart grids (Nazir et al., 2017).

Assumptions, Limitations, and Delimitations

Assumptions

Assumptions are unconscious knowledge, conventions, and socially shared beliefs that may not be real but assumed to be accurate (Atkinson, 2017). My first assumption in this doctoral study was that the open-ended questions in the semistructured interviews would provide an opportunity to explore common themes regarding the strategies used by security managers to prevent security breaches in the SCADA systems' network. I also assumed that the security managers participating in this study would provide honest, open, and unbiased answers to the open-ended questions in the semistructured interviews. The last assumption was that the sample of participants would represent the security managers under study.

Limitations

According to Richardson (2018), limitations are influences outside the control of the researcher, which could disrupt the trustworthiness of the findings. The first limitation of this study was that potential participants or researchers might introduce bias in a qualitative research design (see Sprague et al., 2017). According to Galvin (2015), standardized questions can be used for all participants to counter bias. Hence, I used the interview protocol to remove bias during the data collection process (see Appendix A). I also used member checking to verify the collected data for accuracy, thereby eliminating any bias I may have introduced in my interpretations of the data. Another limitation may be the constraint of the information shared by the security managers due to the privacy and security necessary for SCADA systems. To this end, I received the approval and consent of each partner organization before the commencement of the interview. Also, I adhered to the Belmont Report protocol and assured the participants of the protection of their autonomy, dignity, and privacy.

Delimitations

Delimitations are the borders or boundaries guiding a research study (Kongnso, 2015). The first delimitation of this study is that the sample population came from target oil and gas organizations in the midstream sector located in the Southwest region of the United States. Another delimitation was that the data collection instruments only included semistructured interviews with security managers of the sample companies and a review of their organizational documents. Finally, the sample size of six SCADA systems security managers may be relatively small since a large sample size may add to the interviews' time and cost.

Significance of the Study

Contribution to Information Technology Practice

Organizations that use SCADA systems to control their infrastructure may use the information from this study to manage cybersecurity risks associated with the SCADA system effectively. Cherdantseva et al. (2016) stipulate the need to manage cybersecurity risks in SCADA systems effectively. SCADA security managers may use data collected from this study to identify best practices for dealing with the SCADA systems. It may also help them minimize or secure their SCADA systems' network from cyber-attacks. SCADA security managers may use the findings of this study to prevent data breaches that may occur due to cyber-attack, which, in turn, may prevent the loss of critical infrastructures and help reduce the financial loss organizations may experience.

Implications for Social Change

The implication for positive social change may include preventing malicious consequences such as loss of lives, damage to the environment and economy that may occur with the execution of a malicious command to start or shut down a pump in a pipeline that carries oil and gas. Presumably, the prevention of disastrous consequences for the economy, national security, and public health with the downtime of these systems. The damage that may occur to the environment due to oil spills may also include damage to the waterways, plants, marine life, or service delivery failure, affecting the people within the territory served.

A Review of the Professional and Academic Literature

In this qualitative study, I identified the strategies security managers used to prevent security breaches in SCADA systems' networks in oil and gas organizations in the midstream sector within the Southwest region of the United States. I examined the strategies used by the security managers using a multiple case study design. While guiding the research study using the following research question: What strategies do SCADA security managers use to secure SCADA systems' networks to prevent security breaches? I anchored the literature review on the GST. I used the GST as the conceptual framework to explore the strategies used by security managers to prevent security breaches in SCADA systems' networks. The literature review included the following four key areas (a) GST, (b) security attacks in the SCADA environment, (c) securing the SCADA environment, and (d) the roles of SCADA security managers.

The current literature review provided a basis for this study due to the gaps discovered in the literature, especially related to SCADA security managers preventing security breaches in the SCADA system's networks. I examined GST, the conceptual framework used in this study, the development of the theory, the evolution of the theory, analysis of supporting and contrasting theories. The activities of malicious attackers and the different types of attacks on the SCADA systems were critical points discovered in the literature related to the study (Nazir et al., 2017). Other significant areas included different forms of network attacks on SCADA systems, which involve several protocols (Ghaleb et al., 2018). Ideas related to security mechanisms such as authentication, intrusion detection, logging, event management, and incident response, according to Zhou et al. (2018b), and preventing security breaches on the SCADA systems' networks has been explored but underexplored by researchers. Finally, I also examined the roles played by SCADA security managers in preventing security breaches in SCADA systems' networks.

Literature Search Strategy

I reviewed the extant literature on securing SCADA systems using peer-reviewed articles and journals, dissertations, books, and websites. I used 295 literature review resources, with 86% of the articles published between 2016 and 2021. Ninety-eight percent of the literature review resources were peer reviewed. I summarized these literature review resources in Table 1 below.

Table 1

Statistics for References in the Literature Review

Category	Result
Total number of references	295
Total number of references published within the last 5 years	254
Total number of peer-reviewed references	285
Total number of doctoral dissertations	4
Percentage of peer-reviewed references including dissertations	98%
Percentage of references published within last 5 years	86%

I performed a comprehensive search of the following databases for this literature review: (a) Academic Search Complete/Premier, (b) Emerald, (c) EBSCOhost, (d) Google Scholar, (e) ProQuest Central, (f) U.S. government websites, (g) Walden University Library, and (h) Sage Premier. These databases contained books, conference proceedings, dissertations, magazines, and peer-reviewed scholarly articles. For the scope to be narrowed and find resources that are relevant to this study, the following phrases or keywords were used in the search criteria: *SCADA systems, SCADA security, industrial control system, information security, data breaches, information assurance, information security, GST, SCADA systems breaches,* and *industrial control systems' breaches*.

The General Systems Theory

In this qualitative multiple case study, I explored the strategies security managers used to prevent security breaches in the SCADA systems' networks. I used GST in this study as the conceptual framework to show how organizations will achieve their objectives using the information strategies presented. Bertalanffy (1972) first proposed GST in 1946. The GST was the framework used by researchers to explore the interrelationship between objects working together to achieve specific results instead of working in isolation. Therefore, GST is a robust framework used to understand the wholeness of organizations when all parts within a system work together to accomplish their objectives (Simola, 2018). When a part of the system fails, according to Mar (2019), it may prevent the entire system from functioning as desired.

Bertalanffy (1972) identified three main concepts central to the GST to include: (a) the complete system is larger than the sum of its part, (b) the nature of the components of a system is defined by the whole of the system, and (c) behaviors and theories used in describing a system apply to other systems. Further work of Bertalanffy expatiated that examining systems and how they interact may better explain complex and dynamic systems. Some of the fundamentals of systems theory mentioned by Ofori-Duodu (2019) included (a) objects within a system, (b) attributes of the system and object, (c) the interdependence between objects within the system, and (d) the existence of the system within an environment.

GST applies to this study because SCADA systems are themselves complex systems with a high level of automation that assist in solving control systems development, transmission, storage, processing, and display of information. According to Abraham and Nair (2018), information security is one of the critical elements of an organization crucial to its long-term success. Pieters (2017) emphasized the notion of causal insulation of technological systems from their environment using systems theory. Pieters stated that a protective boundary would ensure that technology functions as designed, implying that unwanted causes are kept outside the system. I used the same lens to explore the best-suited strategies to prevent security breaches in SCADA systems' networks. The unwanted causes include malicious external and internal attackers, vulnerabilities in the systems, and how to insulate the systems.

Evolution of GST

GST has evolved significantly since its original author and various researchers since it is applicable in other fields. Bertalanffy (1972) initially developed the theory to establish an overarching means of holistically describing and understanding the concept of system organization (Rousseau, 2017). According to Drack and Pouvreau (2015), GST was generally applicable to biology and physics. GST has evolved into a more general view of system behavior. A core tenet of GST is that all living things have an organization as an essential characteristic. The organization must be considered a whole rather than as individual entities (Bertalanffy, 1972). Lollai (2017) stated that (a) hierarchic order is another fundamental element of GST; (b) systems are ranked according to their levels of increasing complexity, both in functions and structures; and (c) systems can show new features or emerging properties not exhibited at each level of complexity. Demetis and Lee (2017) elaborated more on the relationship between systems and environments, explaining that systems at all levels have the same characteristics, reinforcing the idea that each complex level is self-contained and distinct.

Complex systems are systems made up of large numbers of distinct objects driven by nonlinear interactions with the environment and between their components (Pascual-García, 2018). The complex system emphasizes holism, which assumes that parts of a whole are intimately interconnected, and they cannot exist independently of the whole. There is a necessity to explore how the various components interact and how to control them. There are three approaches to complexity, according to Soliman et al. (2018). The first approach is the attribute view, which is the most used approach. It assumes that the complexity of a system is attributable to change, the number of parts and interconnections, and dynamism. The second approach involves defining complexity measures equivalent to the amount of data required to reproduce the system. Finally, the third approach assumes complexity to be an emergent characteristic of socio-technical systems. Although GST initially applied to biology and physics, the theory is now applicable to the IT field. GST was used as a lens to explore the effect of social perceptions on IT privacy practice (Pieters, 2017). An adapted version of the GST called sociotechnical systems theory was used, according to Li et al. (2019), to explain the relationship between social aspects and technology at the workplace. The evolution of GST has allowed the inclusion of social, human, organizational factors, and technical factors while designing organizational systems. The addition of human components through GST evolution has direct applications to this study because it is possible to leverage the observed behavior of a human component in one system to apply or modify another.

The dynamic nature of the GST made it possible to adapt it quickly and logically to other disciplines. According to Mazzei et al. (2017), the behavior of various types of systems such as social systems may be described, studied, and controlled by other researchers due to the evolution of GST. I considered multiple aspects of organizational culture and control with their effects on securing the SCADA systems as part of the implementation strategies in this study. According to Mazzei et al. (2017), organizations interact with other external systems such as other organizations or customers. The description of the organization above refers to the interaction of the SCADA systems with the field devices through smart communication technologies such as networks, links, and operators. The adaptation of these smart communication technologies undoubtedly exposed the system to cyberattacks. GST, therefore, provided the framework that allows for an iterative understanding of the system under study.

Application of GST

The welfare and growth of our society depend on protecting and improving the critical infrastructure since their destruction or incapacitation may have a debilitating impact on national economic security, national security, national public health, and safety. U.S. Department of Homeland Security (2016) defined 16 critical infrastructure sectors which include: chemical processing, commercial facilities, communications, critical manufacturing, dams, emergency services, energy, financial services, food and agriculture, government facilities, health care, information technology, nuclear reactors and waste, sector-specific agencies, transportation systems, and water systems. According to Wang et al. (2018), these critical infrastructures are complex because of their interdependence and interconnection with other systems. The essential services rendered by these critical infrastructures are high. The disruption of any of the services may result in the interruption of other services because they are all linked together. For example, a disturbance in the energy sector will affect all other sectors because all other sectors depend on energy to power them.

The SCADA systems remotely monitor and control critical infrastructure processes such as water and waste control, oil and gas refining, telecommunications, energy, nuclear reactors, and transportation (Shitharth & Winston, 2017). The use of SCADA systems with these critical infrastructures facilitates remote access to real-time data monitoring and the command-to-field or remote devices' execution. Therefore, the SCADA systems are vital to the services provided by these critical infrastructures daily. The security of the SCADA systems must be monitored and maintained to mitigate potential cyberattacks. Due to the criticality of cybersecurity for SCADA systems, this study seeks to answer the following research question: What strategies do SCADA security managers use to secure SCADA systems' networks to prevent security breaches? The GST is the lens that I used in this study to explore the strategies used by security managers to secure SCADA systems' networks to prevent security breaches.

As Bertalanffy (1972) described, the systems theory is studying the interdependence of all modules within a system rather than modules working in isolation. The GST is a central theory used in investigating systems because of the interaction of the subcomponents within the system (Bridgen, 2017). From a general systems theoretic perspective, the focus is on the interactions between subsystems that made up the

SCADA systems. The subsystems that made up the SCADA systems, according to Zhou et al. (2018b), consists of the control center, wide area network (WAN), and the field site. The control center consists of the SCADA server master terminal unit, communication routers, HMI, historical databases, and engineering workstations. A local area network connects these components.

According to Maglaras et al. (2016), the purpose of the control center is to collect and record the latest information from the remote units, display the information using the HMI, and generate action based on the detected events. Other responsibilities of the control center include trend analysis, central alerting, and report generating. The field site consists of PLCs, Intelligent Electronic Devices, RTUs, modems, and WAN cards. The field site is responsible for controlling the actuators and sensors. Remote repairs and diagnostics are possible because the field equipment can be remotely accessed using a WAN connection. Information transfer between the field sites and the control centers uses standard and proprietary communication protocols using telemetry technologies such as cables, fiber optics, and radio frequencies such as microwave, radio, and satellite.

According to Bertalanffy (1972), the GST views a system in its entirety and the relationship between all the different subsystems that made up the whole system. Zoto et al. (2019), and Markovic-Petrovic et al. (2019), in a study of a new method for assessing security risks in SCADA networks, took an in-depth look at three phases: objective, subjective, and final assessments. These phases have clear benefits of precise risk assessment and a higher return on security investments. The objective phase considers SCADA historical data, such as parameters that describe the state of a process concerning attack threats. In the second phase, consideration for outputs from experienced SCADA experts such as security managers. Finally, the third phase combines the outputs of the two previous phases to obtain a final risk assessment. Likewise, this study intends to explore the interactions within the subsystems that made up the SCADA systems, obtain insight into the effects the subsystems have on each other, as well as the whole system. The experience of SCADA security managers would also be considered in combination with the insight into SCADA systems to prevent security breaches.

The systems theory is distilled into six requirements that illustrate the fundamental concepts of the vast theoretical landscape, according to Schultze (2017). Highlighted below are the six key concepts:

- *The whole is much more than the summation of its parts*. The interaction of components creates a new substance, implying that it generates a new element when the same component interacts with another element.
- *Goal seeking*. A final goal is achievable when subsystems interact among themselves.
- *Transformation*. The processing of inputs and outputs is the fundamental mechanism by which systems achieve their goals. Systems are hierarchically decomposed into subsystems due to the complexity of this operation.
- *Self-reference and autopoiesis*. Autopoiesis refers to the ability of the system to reproduce itself. This regeneration relies on information about the system to self-correct and reproduce itself.

- *Environment/system distinction*. The environment is constitutive of the system even though it is external to it.
- *Communication*. This process includes the utterances that send information to another system and the understanding achieved by the utterance's targeted entity.

These six essential requirements explained the interdependence and the dynamic relationships between components of the system. A system is established based on the patterns and the relationships emerging from the interactions among the different subsystems. As the SCADA system can be seen as a mega-system consisting of subsystems, GST, according to Katrakazas et al. (2020), provides the opportunity to address the various challenges faced on the micro-level and on the macro level. GST served as the guiding framework for investigating and managing the micro and macro levels of the interactions inside the SCADA systems.

The goal of systems theory, apart from these six essential requirements, is to tackle complex phenomenon built through the combination of more extant components (Schultze, 2017). Also, Schultze (2017) noted that systems theory's contingent construction of observation ensures that understanding differences in meaning is possible using observer-relative distinctions by observing the observer. The complexity of events occurring within a system depends on the limitations and the observer's view. As the observer of the participants, I did not take the first impression as the complete picture; therefore, I challenged them by asking further questions and seeking interpretations and descriptions of the phenomenon under study.

The systems theory consists of the following critical components include: (a) objects within a system, (b) attributes of the system and object, (c) the interdependence between objects within the system, and (d) the existence of the system within an environment (Ofori-Duodu, 2019). Similarly, in my doctoral study, (a) the organization and the SCADA systems are the objects, (b) SCADA systems' network security management strategies are the attributes, (c) the geographically dispersed SCADA systems used for monitoring and controlling industrial process equipment in Realtime represents relationships, and (d) the Realtime and the historical data contained within the organization represents the presence of a system within the environment.

The SCADA systems were designed to be robust, open, easily operated, and repaired but may not necessarily be secure (Alves et al., 2018). The security of SCADA systems is of great concern because of its exposure to cyberattacks from the internet. This study explored and understood the relationship between the various components of the SCADA systems, networks, the internet, malicious attackers, and security breaches. The GST served as the lens for exploring the strategies used by security managers to secure the SCADA systems' network from security breaches. The complexity of the SCADA systems and its cyber threat landscape continues to evolve and results in some challenges faced by compliance professionals and security managers. Cybersecurity is an enduring challenge faced by the IT discipline (Shoemaker et al., 2017). Therefore, I adopted a holistic perspective to explore the various relationships between the various components of the SCADA systems, the networks, malicious attackers, security breaches, and the strategies used by security managers to prevent breaches.

The GST provided a framework for investigating and defining systems and their phenomena free from biases. GST allowed the concept under review, values, and other related entities to be explicitly defined and discussed in detail. Using GST as the conceptual framework, the idea of security, control, and communication of the SCADA systems was investigated, explained, and defined on an accessible level from any biases other than the system concept itself. The threat to the functioning of one or multiple components of a system constitutes a threat to the operation of the whole system (Mar, 2019). GST offered a scientific framework for developing measures to improve the stability and security of both the different components and the whole system.

The SCADA systems can be viewed as a subsystem of a more extensive system, in this case, the organization. To better understand the role of the SCADA systems and fully appreciate how GST may be used in this study, understanding the organization is required. According to Hartnell et al. (2019), the organization consists of leadership, structure, strategy, and high-performance work practice that are highly interdependent. Based on this definition of the organization, the SCADA system is a control system or a subsystem that helps accord common purpose within the more extensive system. The common goal within the larger system can only be accomplished if all the interdependent elements function as they should. According to Abraham and Nair (2018), information security is crucial to the long-term success of an organization.

System theory represents a better approach to exploring how elements within a society are linked and how the relationship between them evolves. According to Caputo et al. (2019), the GST approach supports (a) the shift from a mechanistic and reductionist approach to the composition of elements and their relationship with a dynamic and holistic view, where the focus is on the elements that affect the whole phenomenon, and (b) a better understanding of how an entity can organize itself by sharing resources with the external environment to achieve conditions of survival. Concerning the above perspective, the GST offers an opportunity to define a conceptual framework that effectively links the social and technological dimensions. Caputo et al. (2019) opined that enlarging the perspective in social and technological studies will build better bridges among technical instruments and human resources.

The use of technical instruments alone is not enough to secure SCADA systems. According to Ani et al. (2019), technology is weak and vulnerable, just like the people who developed and operated it and the process of making use of it. Advanced technology is not smart in solving issues, but it may become smart when aligning with its ability. Systems theory stressed the importance of considering individuals within their broader environment against studying human behavior in isolation (Alfandari, 2019). Socio-technical systems theory advocates that all stakeholders, such as end-users, designers, managers, clients, and human resource experts involved in a given system, should be included in the design, development, and implementation processes (Hughes et al., 2017). When all the stakeholders are involved, they will clearly understand the system design and operation, which will result in more effective systems, and better designs. Adaba and Kebebew (2018), in a study to improve the health information system of national health service hospitals, considered social, technical, and organizational factors and the interactions between the different stakeholders.

The SCADA systems have evolved towards adopting cloud computing and the Internet-of-Things due to technological progress and the need to improve its efficacy and functionality. A wide range of security vulnerabilities introduced to the SCADA systems is due to existing implementation and practice (Qassim et al., 2019). The systems have become an obvious target for cyberattacks. These attacks range from service disruption to damaging critical operations, leading to economic losses or loss of lives. Therefore, it is imperative to identify and analyze the weaknesses and vulnerabilities of these systems. GST played a vital role in this analysis to develop proper security solutions and protection mechanisms.

Cyberattack threats are evolving as technology also changes, thus requiring effective detection and protection measures. According to Qassim et al. (2019), three countermeasures are necessary to secure SCADA systems. The first countermeasure is identifying all known security incidents around the systems using security tools such as firewalls and intrusion detection systems (IDSs). Secondly, look into the normal functioning of controls in the SCADA systems network and analyze the flow of data in the system to identify threats attempting to damage or alter the system. Lastly is the integral approach, which involves conducting technical auditing tests such as penetration tests to eliminate the SCADA systems design and implementation vulnerabilities.

The rationale for adopting GST in this study was to improve the chances of understanding the complexity of the interdependent subsystems that made up the SCADA system. GST and its principles provided a comprehensive, inclusive, and open framework to study the complexities and the dynamic nature of the SCADA systems and the strategies security managers used to prevent breaches in the systems' networks. Although GST may not be the ultimate panacea to the security problems in the SCADA systems, it provided a basis to help organize the system.

Supporting Theories

It is possible to use many theories to research the strategies security managers used to prevent security breaches in the SCADA systems' network. But a researcher must determine if a chosen theory will assist in answering the central research question. I chose GST for this study as the conceptual framework due to the nature of the study to help understand the phenomenon.

High-Reliability Theory

One of the supporting theories was the high-reliability theory (HRT), which emerged from the desire of three original researchers, La Porte, Roberts, and Rochlin, in 1984. La Porte, Roberts, and Rochlin desired to understand the ability of organizations to operate effectively and manage complex and intrinsically hazardous technical systems (Rochlin, 1996; Rochlin et al., 1998). HRT was not selected because it involves studying organizations staying within the safe envelope and avoiding accidents under challenging conditions. In contrast, GST encourages researchers to view an organization and its environment as one whole and not as individual entities (Bergström et al., 2015; Phipps, 2019). Organizations with excellent safety culture or high-reliability organizations (HROs) are other terms used for the phenomenon. One of the attributes of HROs is that they are not bound to organizational routines built on the past, but they continuously revise and change their expectations (Grabowski & Roberts, 2019). HRT involves studying how the complexity of modern socio-technical systems makes them inherently risky and how to adapt to the emerging risks to guarantee the system's success (Saunders et al., 2016). GST involves understanding the wholes that consist of interacting components (Stefano, 2017). Although GST and HRT involve complex systems, and the difference between the two is that HRT deals primarily with nuclear power plants, aircraft carriers, and air traffic control (Grabowski & Roberts, 2019). GST encompasses many disciplines under a system-based approach and a unique, wide-ranging framework (Stefano, 2017).

Technology Threat Avoidance Theory

Another theory that was not chosen but considered for this study was the technology threat avoidance theory (TTAT), which researchers use to evaluate how systems exposure may trigger malicious threats. Liang and Xue developed the theory to demonstrate the reaction of computer users to perceived threats to systems' infrastructure. The theory encompasses many disciplines, such as risk analysis, psychology, health care, and information systems (Liang & Xue, 2009). According to Chen et al. (2018), the theory may be employed by investigators to explore employees' negligence of organizational policies and inappropriate use of network resources, passwords, computers, and email. The negligence of organizational policies on the part of the employees may be detrimental to the corporate information systems. Organizations may avoid malicious threats by using safeguarding measures such as antivirus, firewalls, voice analysis, biometric devices, and other authentication devices. According to Chen and Liang (2019), TTAT has proven to be a helpful lens by several empirical studies to assess individuals' coping behavior when encountering various IT threats. With TTAT, users access threat levels only when under attack and appraise whether the threats are avoidable with the current safeguarding measures. From cybersecurity's perspective, it would leave the systems exposed to cybersecurity risks. As opposed to TTAT, GST could view systems and their elements holistically while also considering the socio-technical aspects.

Contrasting Theories

Apart from using the theories mentioned above to research the strategies used by SCADA security managers to secure SCADA systems' networks to prevent security breaches, there also exist theories that are in contrast to GST, the selected theoretical framework.

Grey Systems Theory

One of the contrasting theories is the grey systems theory developed by Professor Deng in 1982 as a quantitative method for dealing with partially known and unknown information (Deng, 1982). According to Sifeng et al. (2016), Grey systems theory requires inadequate information and small samples. Therefore, the researcher must make assumptions based on incomplete information to reach conclusions. In the context of this study, SCADA systems are complex and consist of large numbers of distinct objects driven by non-linear interactions with the environment and between their components (Pascual-García, 2018). The grey systems theory contrasts with GST since the relationship between the distinct objects within the system cannot be adequately analyzed if the required information is incomplete or inaccurate.

Crime Pattern Theory

Another contrasting theory to GST is the crime pattern theory (CPT), which was introduced in 1981 by Brantingham and Brantingham to demonstrate how offenders determine and identify their targets (Brantingham & Brantingham, 1993). The theory studies the behavioral pattern of individuals during their day-to-day activities to help understand how targets are identified and chosen (Welsh et al., 2018). Crime does not occur randomly; they are planned by the perpetrator or due to a presented opportunity. According to Weisburd (2015), the main elements of CPT are nodes, paths, and perimeter. Individuals referred to as nodes consist of everyday life locations such as home, school, work, and entertainment areas. The routes taken to and from these nodes are personal paths, while the perimeter is personals paths that connect with different nodes (Weisburd, 2015). According to Welsh et al. (2018), CPT determines how to choose opportunities based on the target selected by an. In contrast to GST, CPT focused upon prevention and an organized way of exploring behavioral patterns (Welsh et al., 2018). It does not analyze the other elements such as the offender, targets, nodes, and personal paths. Whereas GST observes phenomena under review as a whole and not as a separate entity (Phipps, 2019).

GST was ultimately chosen as the conceptual framework to drive this study for the following reasons. First, GST is the study of wholes and wholeness, and the phenomenon under review should be observed as a whole and not as a separate entity (Phipps, 2019). The organization system is a purposeful interrelated subsystem working together to accomplish a common goal. A failure of one of the subsystems may lead to the collapse of the whole system. Secondly, the phenomenon under study meets the criteria of being classified as an open system; therefore, I applied GST to the target organizations. Lastly, the use of the technical approach to cybersecurity risks only addresses a subset of the problem. Cybersecurity requires a holistic approach; hence, GST encourages a holistic approach. It was used as the lens to view the strategies security managers used to prevent security breaches in SCADA systems' networks (Rousseau, 2017).

Security Attacks in the SCADA Environment

Cyberattacks of the SCADA system come in various forms that are harmful to the system. According to Torten et al. (2018), the objective of cyber attackers is to attempt to install ransomware, steal unauthorized information, and violate intellectual property. Cyberattacks may be impelled socially or politically and may be delivered externally or internally (The council of economic advisers, 2018). The continuous integration of the SCADA systems to sophisticated technologies gave birth to a new breed of cyberattacks (Genge et al., 2019). According to Zhou et al. (2018a), the SCADA system consists of four components: a business network, monitoring network, control system, and field system. The business network provides policymakers with information, and they include business services such as mail servers and the webserver. The monitoring networks bridge the business networks and control systems, mainly the SCADA systems, historical databases, and historical records (Zhou et al., 2018a). The control system consists of the HMI, Intelligent Electronic Device, RTU, and PLC. The bottom of the entire SCADA system is the field system, mainly used for executing the control commands issued by the operating system.

Business networks are the easiest to attack due to their connection to the internet (Zhou et al., 2018a). They also provide many services, such as mail servers and web servers, which increase the attack surface (Myers et al., 2018). Monitoring networks are vital to the safety of the SCADA systems since they create a bridge between the business networks and control systems (Maglaras et al., 2016). The monitoring network is affected if the business network is compromised. The fragility of the monitoring network, such as unmanaged assets, weak passwords in historical databases, and thin firewall rules, may increase the attack surface (Zhou et al., 2018b). Severe physical damage may result if the control system, which directly controls the field devices, is compromised. Some of the attack surfaces of the control system include weak firewall rules, insecure protocols, unencrypted data transmission, and insecure wireless transmission (Zhou et al., 2018b).

Apart from external attacks on the SCADA systems, the system may also be attacked internally by insiders. One of the most expensive security concerns for business organizations is the insider threat since they do not foresee the malicious activities of these internal individuals (Callegati et al., 2018). Insiders are more familiar with the system, and as such, they have more advantages than outside hackers. Motivation and opportunity play essential roles when information security rules and regulations are violated (Safa et al., 2018). According to Homoliak et al. (2019), insider attackers may hold a grudge against the organization or be financially motivated.

IT Security

System security is essential for all organizations that require information systems in their operations. System security issues are not new, but there is a need to develop new approaches to protect systems from cyberattacks necessary because of advancements in technology (Ashibani & Mahmoud, 2017). Zhong et al. (2018) stated that organizations implemented various automated defense measures such as IDSs, vulnerability scanning tools, antivirus software, security information, event management, and firewalls to protect their critical information infrastructure. Sawyer and Hancock (2018) asserted that cybersecurity is the teaming of humans and automation, and both humans and machines are vulnerable to cyberattacks.

Attackers are using various means to launch cyberattacks, primarily through the use of social networks. According to Feng et al. (2019), the social network behavior of users provides means for attackers to launch targeted attacks either accidentally or intentionally. The Achilles' heel of information systems is hardware and software vulnerabilities (Schuster et al., 2017). The majority of hardware and software products consist of exploitable vulnerabilities. Preventing these vulnerabilities by adding security in the design from the start may considerably increase the protection level.

SCADA Systems Security

New challenges in providing cybersecurity for the SCADA systems in critical infrastructure occurred because of the system's move from the isolated legacy system to traditional information technology (IT) networks (Rodofile et al., 2019). The security of the SCADA system is essential because of the expectation of the services provided to be always available (Kalech, 2019). The BlackEnergy attack that targeted the Ukrainian electricity grid left vast populated regions without electricity (Genge et al., 2019). SCADA components such as sensors, PLCs, RTUs, and HMI communicate through dedicated protocols like Modbus, XModbus, Open Platform Communication, and ABCIP (Martín-Liras et al., 2017). Sensitive data are transmitted through these components to the master station through network interfaces, communication equipment, software, and input and output devices (Myers et al., 2018). Organizations can remotely or locally manage industrial processes; gather, monitor, and process realtime data; interact directly with devices such as pumps, motors, valves using HMI software; and create log files of events (Alves et al., 2018). Therefore, it is imperative to know the risks involved in using SCADA systems and implement adequate protective strategies.

In the first use of the computerized SCADA systems, there are little or no security features embedded into the systems (Rosa et al., 2019). Security by obscurity had been the primary security methodology used. According to Kalech (2019), protecting the systems from a malicious entity is possible using non-standard protocols and devices since they will not know how to attack it. The concept of security by obscurity is still in use, according to Kalech (2019), due to the following reasons: (a) The lifecycle of the SCADA systems is generally around twenty years, and the SCADA systems personnel are mostly engineers that are not security conscious. (b) There is no off-the-shelf security software for the systems' components because the systems are different from one another. (c) SCADA systems cannot be unavailable in contrast to IT technology; therefore, SCADA security managers are skeptical of installing security devices that may harm their operations.

The growing connectivity of the SCADA systems to the internet and the lack of adequate security for the systems have exposed it to the attack vectors used in most cyber-attacks (Bhamare et al., 2020). Enormous physical damage and human life danger may occur if the SCADA systems are compromised. Therefore, securing the system properly from cyberattacks is essential, and the users of the systems must understand the inherent security issues and know the roles of securing the systems. Dreier et al. (2019) emphasized the integrity and availability of SCADA systems, while the security objectives for IT systems are confidentiality, integrity, and availability (CIA). The availability of the SCADA system is crucial because dramatic consequences may result in a lack of timely information to and from the field, especially when the field devices are unable to receive an adequate command.

Securing the SCADA Environment

The SCADA system is different from the traditional IT systems because they use various protocols such as MODBUS, EtherNet/IP, and Distributed Network Protocol version 3 (DNP3) (Huda et al., 2018). According to Kalech (2019), these protocols interconnect with PLCs, RTU, HMI, sensors, and actuators. The design of the current antimalware tools is with the behavior of executable files in mind, which focused on application program interfaces (APIs) and operating system (OS) calls (Huda et al., 2018). These anti-malware tools are more suitable for safeguarding systems and applications operating under the corporate network, which uses APIs and OS calls. In contrast, the data communication between HMIs, RTUs, and physical devices happens most, especially on physical, data, and application layers (Huda et al., 2018).

The main objective of this study was to explore the strategies used by security managers to secure SCADA systems. Three main strategies were classified by Forde (2017) as follows: informal, formal, and technical. According to Ani et al. (2019), most security solutions deployed are technology inclined while neglecting people and process security context. The SCADA systems are built and operated by people for executing processes. Only a fraction of the more significant security problems of the systems is taken care of through securing technology (hardware and software). Ani et al. (2019) explained further that technology is as vulnerable and weak as the people who developed and operated it and the processes designed to use it. Therefore, the combination of informal, formal, and technical strategies is essential in securing the SCADA systems.

Technical Strategies

Organizations deploy technical security measures (TSMs) to protect themselves from cyberattacks and data breaches (Molin et al., 2018). More stringent security measures will result in higher levels of security with the use of these TSMs as intended by employees, although productivity may have a negative impact. TSMs include biometric devices, antivirus, digital signatures, firewalls, and other authentication protocols to protect the information system against cyberattacks (Gcaza et al., 2017). Key management and encryption, entitlement, identity, access management, data security, and information management are other methods to implement TSMs. Disaster recovery would be necessary if all these methods failed.

Key Management and Encryption

Key management and encryption are essential for encrypting data to reduce data leakage. According to Zhou et al. (2019), encryption ensures data protection in modern cryptography. The National Institute of Standards and Technology (NIST) advised in 2015 that the design of SCADA systems should incorporate encryption and authentication between devices (Qian et al., 2019). It would be tough for hackers to reverse engineer protocols and forge network packets on the control system. But according to Radoglou-Grammatikis and Sarigiannidis (2019), the use of encryption and authorization mechanism may not be enough to prevent various security threats, especially the denial of service (DoS) attacks.

The use of end-to-end encryption will help protect data and prevent unauthorized access to information (Qian et al., 2019). End-to-end encryption is a communication method that ensures that attackers cannot access the cryptographic keys required to decrypt a communication (Qian et al., 2019). Therefore, we may utilize end-to-end encryption for data communication between the main stations and RTUs with Ethernet (Leszczyna, 2018). End-to-end encryption is an efficient way of protecting data and protocol between the RTU and the controllers. The solution also offers authentication for communication and protection against man-in-the-middle (MITM) attacks and relay attacks.

Another solution proposed is private information retrieval (PIR), which according to Sun and Jafar (2018), is a technique for retrieving a single message from many messages without letting the database server know the extracted message. But according to Lai et al. (2018), the traditional PIR must first publish the description of each data item stored in the database for the user to choose from before running the protocol without revealing the content of each data item in the process. Lai et al. (2018) proposed attribute-based PIR to enhance data privacy to eliminate information leakage of the data item during the PIR system. Another approach proposed by Harlow (2018) is the public/private key infrastructure (PKI); if deployed as an additional point of verification between system components and numerous gateways, it would take the most potent computers decades to crack at light speed.

Information and Communication Management

Cyberattacks are now a significant threat to the internet world. According to Mohamed (2017), the move of the SCADA systems from proprietary technologies to open and standardized solutions and their connections with the office networks and the internet has exposed them to the vulnerabilities common to computer security. Since these systems play vital roles in critical infrastructure, designing more secure SCADA systems from increasing and unpredicted cybersecurity threats is vital. Therefore, accidental or intentional manipulation of the system may have severe consequences on the economy, society, and the environment. The integrity and authenticity of the SCADA messages are vital to the system's security (Cherifi & Hamami, 2018). An operator can decide or implement an action only when provided with complete and correct information.

The confidentiality of the information provided is vital as the authenticity and integrity since the system provides real-time information about the managed critical infrastructure. The information may include its state, weaknesses, and activities. According to Cherifi and Hamami (2018), malicious attackers may use this information to determine the appropriate time and ideal type of physical attack. Preserving confidentiality may also protect against passive attacks and maintain the authenticity of the information.

This domain emphasizes the relevance of information and communication management in the SCADA system. According to Ghosh and Sampalli (2019), the usage of cloud computing, internet connectivity, social engineering, and wireless communication on the SCADA systems' networks have made it vulnerable. Ghosh and Sampalli (2019) pointed out two security schemes required to address the security threats to the system as the detection of attacks on the system and prevention of the attacks. Cyber attackers are creating new methods of attacking the SCADA systems, and detecting these further attacks against critical infrastructure may protect human life and assets. Yilmaz and Gonen (2018) opined that the detection of attacks is more important than preventing attacks. It may be possible to prevent attacks on the SCADA systems if detected on time.

Identity and Access Management

Identity and access management (IAM) is best suited for security managers to add their security strategies. Management of computers, users, and other components within the network infrastructure is necessary with the gradual increase in the number of systems within an enterprise. Many data leakages occur due to vulnerabilities in identity management systems (Indu et al., 2018). Kunz et al. (2019) asserted that it is possible to automate users' administration workflow using IAM solutions. The governance of standards compliance requirements is possible with introducing a standardized IAM mechanism, guidelines, and technologies. According to Sindiren and Ciylan (2019), adjustment of users' authorizations will allow them to have access only at the level they are authorized to ensure the integrity and privacy of data stored in the information system. This section focuses on all identity and access types significant for SCADA systems. Kim et al. (2014) considered strengthening authentication processes and user account management. Only the authorized personnel should access the HMI workstations used by the controllers to operate and control equipment, the network devices, and the central servers. Authorized managers and users should perform control access, including the provision of IDs, registration, disposal procedures, and change (Kim et al., 2014). The practice of sharing IDs and passwords among operators should be discouraged and discontinued without exception.

Disaster Recovery and Business Continuity

The SCADA systems monitor industrial processes such as electric grids, oil and gas pipelines, traffic control systems, space stations, water treatment plants, and nuclear systems. The systems, therefore, has to be continuously available because it supports critical infrastructure. Despite the efforts made to secure the systems, there are reports of incidents that may occur due to cyberattacks, human error, or natural disasters. According to Schlegel et al. (2015), it is impossible to achieve 100% security despite all efforts to secure the system and prevent incidents. Therefore, security managers should prepare to deal with incidents efficiently and promptly if they occur. There should be a methodology to investigate and determine the state of files and systems after an incident since the system's availability is critical. Murillo et al. (2018) pointed out that software-defined networks (SDNs) and network functions can make it possible to automatically respond to an incident that may occur from attacks against the SCADA system. According to Murillo et al. (2018), network function virtualization (NFV) and SDNs are technologies designed to improve network capabilities through (a) better management of network visibility, (b) traffic flows, and (c) the control and deployment of network function using software against the hardware-specific middleboxes.

Informal Strategies

The SCADA system is complex, and as such, securing the system is complex. Combining technical, formal, and informal strategies are required to secure the system (Ahmad et al., 2019). Informal strategy, according to Sindhuja (2014), is vital to an organization's security structure. Informal strategies consist of awareness programs to sensitize employees to information security. The awareness may be through cybersecurity training or seminar through which the employees are made aware of both internal and external threats. According to Abraham and Chengalur-Smith (2019), information security best practice awareness is possible within organizations through information security training. Although, employees view information security training as boring and just another item to cross off their checklist. Organizations can tailor the learning process to individual abilities, learning styles, and levels of knowledge. Tailoring the learning process can decrease the learning times and improve the learning outcomes. According to Elifoglu et al. (2018), security training should be conducted for employees as soon as they have a new user account. Current employees and business partners should also receive the same type of training as a new employee at a specific interval. Adequately trained employees would be able to detect and notice suspicious activities.

Formal Strategies

Formal strategies are rule-based, dictating how to utilize technical strategy to manage information security within an organization. According to Li et al. (2019), the formal strategy helps develop policy and procedures, establishing apparent authority within the organization, and facilitating seminars and workshops to train employees. Regulation of inappropriate use of passwords, computers, network resources, and email by employees is possible through information security policy (ISP) (Chen et al., 2018). According to Chen et al. (2018), an organization's information and technology resources are better safeguarded by ISP through a statement of the roles and responsibilities of the employees. The statement of roles and responsibilities should explicitly explain how to use information, resources, systems, and privilege accounts. The statement should also outline the process of dealing with grievances among employees and the consequences of policy violations.

Service Level Agreement (SLA)

The exposure of information systems to various threats may result in different types of damage, leading to financial losses, economic losses, environmental destruction, and even loss of lives. According to Silva et al. (2019), organizations struggle to understand the types of threats that may affect their information assets and mitigate the risks. SLA is a crucial requirement and a contract between a customer and service provider, which defines the minimum set of services that the customer may receive from the service provider (Al-Sayyed et al., 2019). The SLA's successful definition and correct setting are essential (Sodomka & Klcova, 2016). Some of the definitions and settings of SLA include determining the level an employee can access an organization's sensitive information, described in a precise manner, monitoring capabilities, and supervising employees' activities. SLA also governs how employees report suspicious actions of other employees. According to Al-Sayyed et al. (2019), the SLA ensures a chain of escalation of reporting incidents due to insiders or insider threats. SLA also makes provision for authorities that make decisions when incidents occur and the mechanism for managing and taking remedial actions.

Information Technology Governance (ITG) and Oversight

Another formal strategy is ITG and oversight, a structured process that ensures organizations use IT effectively and efficiently to achieve their desired objectives (Borja et al., 2018). Business continuity is affected by many risk factors, and ITG provides an organization with relief for this situation (Rivas-Asanza et al., 2018). The primary purpose of ITG, as explained by Turel et al. (2017), is to create business value and improve organizational performance. The failure of ITG is responsible for IT investment failure and information security breaches (Huygh & De Haes, 2019).

There is a need for organizations to strive for efficient and effective ITG since it enables the preservation and creation of IT business value. Three significant sets of guidance and collective decisions under ITG include focus, scope, and pattern (Gregory et al., 2018). The focus of ITG is on IT-related artifacts and activities that must be in line with business strategies and objectives. The scope of ITG refers to all stakeholders and actors that may be held accountable for ensuring the contribution of IT to the organization. Patterns of ITG are the measures that are put in place to ensure that the outcome of IT-related activities is the desired one. Borja et al. (2018) identified five objectives that must be in place to achieve an effective ITG to include (a) using IT cost-effectively, (b) using IT effectively for growth, (c) using IT effectively for asset utilization, (d) using IT effectively for business flexibility, and (e) using IT effectively to accomplish compliance with legal and regulatory requirements. Organizational units and roles responsible for making IT-related decisions and IT monitoring procedures are part of ITG structures. The ITG structures ensure that daily behavior is consistent with laid down policies.

Risk Management Strategy

The SCADA system is experiencing exponential growth in many industrial fields (Elhady et al., 2019). Due to the considerable increase and development in information technology, the SCADA system is shifting from propriety technology and protocol-based system to an internet-based system. The risks that target the SCADA systems have also increased due to this paradigm shift. Kure et al. (2018) stated that risks are uncertain events due to system failure or malfunction that may harm assets, such as the environment or human beings, and influence the organization's strategic and operational achievement. To effectively protect the SCADA system, a risk management process is required to identify all the risks (Elhady et al., 2019). Elhady et al. (2019) also emphasized the urgency of identifying, evaluating, and treating the various types of threats that may target the SCADA systems. Kure et al. (2018) indicated that risk management is a continuous process and not a one-time event.

According to Kure et al. (2018), risk management is an essential discipline for making effective decisions and sharing the results within organizations. Organizations must make adequate preparations to act against threats and security breaches before their occurrence. The deployment of risk management strategies will ensure the organization quickly recover from security breaches whenever they occur. According to Muratoğlu et al. (2018), cyber risks must be assessed and analyzed parallel with the system engineering process. Continuous tests and fixes should be carried out on cyber vulnerabilities to mitigate cyber risks quickly and cheaply.

A robust and collaborative risk management framework has become urgent to identify, evaluate, and treat the different types of risks targeting the SCADA systems. Elhady et al. (2019) stated that a set of parameters should describe all possible scenarios that may occur and affect the SCADA systems either directly or indirectly. Among the parameters defined by the authors include (a) the risks that may occur to the system, (b) agents who can make the risk happen, (c) motivation or reason for taking the risk, (d) methodologies and penetrations tools used for performing the risk, (e) the targeted components of the system, and (f) vulnerabilities within the element that the agents may exploit.

The Role of SCADA Security Managers

Organizations depend on security managers to protect organizational infrastructure from cyberattacks. Security managers have deployed different security standards to secure communications between nodes of SCADA networks (Ghosh & Sampalli, 2019). According to Shahzad et al. (2016), established global organizations such as U.S. Homeland Security Department, U.S. National Security Agency, the Gas Technology Institute, and the American Gas Association have been vulnerable to security threats due to connectivity to the internet. Cyber attackers deploy different intrusive actions to exploit systems' weaknesses while SCADA security managers implement various security measures to protect SCADA systems (Durkota et al., 2016). The actions of cyber attackers on the SCADA systems are considered severe threats to these systems due to their catastrophic impact and social safety (Lee, & Hong, 2020). A SCADA security manager in an organization may develop a vulnerability assessment framework for securing the SCADA systems, improve authentication and access control management, and ensure systems confidentiality, integrity, and availability. Therefore, organizations require experienced SCADA security managers with the necessary strategies to secure the SCADA systems and prevent security breaches on the systems' networks.

SCADA security managers invest time and resources in securing the SCADA systems while ensuring they meet security requirements. According to Diesch et al. (2020), information security managers must clarify relevant information and consider their interdependencies. Some of the actions taken by information security managers include preventing unauthorized modification and disclosing information, and preventing unauthorized individuals from penetrating their systems (Stiawan et al., 2017). Security managers are entirely in charge of considering and responding to information security issues (Diesch et al., 2020). For example, security managers must consider human behavior and technical threats in the SCADA systems while taking effective and proper actions to mitigate risks.

Information security managers deploy risk management techniques to deal with threats and vulnerabilities that pose risks to organizational information assets (Brunner et al., 2020). Information security risk management ensures that information security risks are appropriately identified, analyzed, and mitigated according to organizational guidelines (Brunner et al., 2020). The end-users hold a vital role in preventing information systems' risks since they are the weakest link in the information security chain of any organization (Dang-Pham et al., 2017). As a result of the critical role played by end-users, organizations could not protect their information systems using technological measures only. A significant number of end-users efforts are required to promote desirable information security behavior and deter malicious activities (Dang-Pham et al., 2017). End-user activities may include interaction with the system, user errors, faults, and user reactions.

Security managers execute effective security incident response strategies to minimize damage from security incidents and learn from such incidents (He & Johnson, 2017). According to Midi et al. (2016), the approach to incident response includes information on preventing attacks, detecting suspicious activities, and monitoring for suspicious activities. According to Choi et al. (2018), recent research attributes information security incidents to humans with malicious intent, lack of knowledge, flawed information security policy, and negligence. He and Johnson (2017) documented incident response security managers can use to minimize damage from security incidents to include (a) preparation, (b) identification, (c) containment, (d) eradication, (e) recovery, and (f) follow-up. The main activity of the follow-up phase is the ability to learn from the mistakes made during the incident handling process. Cyber attackers may launch a series of attacks on the SCADA systems, and the ability to develop an effective response plan will help mitigate against security breaches.

Security managers develop new approaches to protecting their organizational information infrastructure from cyberattacks due to advancements in technology (Ashibani & Mahmoud, 2017). Security managers implement various defensive measures such as IDSs, vulnerability scanning tools, antivirus software, security information, event management, and firewalls to protect their critical information infrastructure (Zhong et al., 2018). Although it is impractical to remove all risks in SCADA systems' networks, security managers could mitigate risks to an acceptable level using technical, informal, and formal strategies (Forde, 2017). According to Ani et al. (2019), technology is as vulnerable and weak as the people who deployed and operated it and the process designed for its use. Security managers' deployment of informal, formal, and technical strategies is vital in securing the SCADA systems' networks. An informal approach involves creating awareness through cybersecurity training or seminar (Elifoglu et al., 2018). While the formal strategy helps develop policy and procedures, establish apparent authority within the organization (Li et al., 2019).

Assessing the vulnerability of the existing system is another role that SCADA security managers should play. According to Upadhyay and Sampalli (2020), field devices such as RTUs, and PLCs are vulnerable to malware attacks due to weak structural design. Most of these field devices were manufactured in a period when cyberattacks were not a significant concern. Stuxnet and Flame events occurred in 2010 and 2012, the attack on a German steelworks control system. The more recent attack on the Ukrainian electricity distribution system demonstrated SCADA systems vulnerabilities (Busby et al., 2017). Security managers need to evaluate and assess the weaknesses of the existing system to determine the robustness and effectiveness of the security mechanisms (Upadhyay & Sampalli, 2020). A better security system may be produced based on IDS and machine learning techniques to protect SCADA systems against malware (Yin et al., 2019).

Transition and Summary

In section 1, I introduced the background of the problem, problem statement, purpose statement, nature of the study, coupled with the research question. I also discussed the assumptions, limitations, and delimitations of the study. Furthermore, I discussed the values that this study might add to organizations in helping them to minimize or secure their SCADA systems' networks from cyberattacks. I also mentioned the positive social benefits that are derivable from the study to include the aversion of disastrous consequences for the national economy, national security, and public health that may occur with the downtime of the systems. I introduced GST, the conceptual framework for the study, which was the lens from which I viewed the strategies security managers used to prevent security breaches in SCADA systems' networks. According to Bertalanffy (1972), GST holistically describes systems and defines them through their functions and various parts. GST demonstrates the impact of interdependent elements such as people, technology, and processes that worked together within organizations to protect organizational assets against the elements working in isolation to achieve the same objective. GST applies to both small- and large-scale organizations focusing on interdependent subsystems working together in a complex system.

The review of the academic literature included the following four key areas concerning the research question: (a) GST, (b) security attacks in the SCADA environment, (c) securing the SCADA environment, and (d) the roles of SCADA security managers. The literature review focused on cybersecurity topics, especially related to the SCADA systems, vulnerability and resiliency of the system, strategy, training, human factor, and compliance. Weaknesses within the SCADA systems' networks may permit cybercriminals to attack and penetrate the systems. It is, therefore, imperative that security managers assess systems faults, evaluate vulnerability and deficiencies of the existing systems to be able to implement appropriate measures.

Section 2 provided added information on the role of the researcher, especially in the data collection process. Furthermore, I discussed the established guidelines for selecting the study participants, research methods and design, population and sampling, considerations for ethical research, data collection instruments, techniques, analysis, and factors associated with the reliability and validity of the study.

Section 3 includes presenting the study's analytical findings and revealing themes associated with strategies security managers used to prevent breaches in SCADA systems' networks. The section also described the application for professional practice, implications for social change, recommendations for actions, further research, and reflections.

Section 2: The Project

In this section, I discussed the project. In the subsections, I addressed the researcher's roles in the data collection process, the participants, and I identified and justified the research method and design. I also explained the population and sampling and discussed ethical research to include an informed consent process. Other information presented in this section consists of the data collection instrument and technique, data organization technique where I discussed the system used to keep track of data, data analysis process, and how I addressed the study's reliability and validity. The subsection is the transition and summary.

Purpose Statement

The purpose of this qualitative multiple case study was to examine the strategies used by SCADA systems' security managers to secure SCADA systems' networks to prevent security breaches. The target population consisted of SCADA security managers who have strategies to secure SCADA systems' networks. I selected the SCADA security managers required for this study from oil and gas organizations in the midstream sector in the Southwest region of the United States. The implication for positive social change may include discouraging attackers with malicious intent from triggering a breakdown in critical infrastructures that keep the society functioning, such as electrical systems, oil and gas pipelines, and water distribution systems.

Role of the Researcher

The role of a researcher in qualitative research is vital and instrumental to the collection of data in the study. According to Sprague et al. (2017), the researcher participates in the study directly influencing the collected data. I was the principal data collector for the study as the researcher. Researchers are to display skills and comprehensiveness during data analysis (Leedy & Ormrod, 2015). I was also responsible for analyzing the collected data and interpreting the analyzed data in an unbiased manner. According to Sprague et al. (2017), researchers may introduce bias into research work. I focused all efforts on removing biases during the study's data collection process by leveraging an interview protocol during the process. I concluded the interviews once I attain data saturation. I also played other roles to outline the scope, limitations, assumptions, and research boundaries. Amongst the data collection instruments that I used in this study are semistructured interviews conducted with open-ended interview questions. I did not conduct interviews in person, while I conducted all using a remote communication medium such as Zoom and Microsoft Teams.

I selected participants for this study from oil and gas organizations in the midstream sector in the Southwest region of the United States. Some of these companies are direct customers of my organization. Still, I did not have a direct relationship with the SCADA security managers of the companies. My responsibility, as the researcher, was to ensure that the results of my study are not affected by the relationship I have with these companies by ensuring the potential participants do not have a previous working relationship with me to prevent potential bias in their responses. I only used the relationship I had with these organizations to help find participants willing to participate in this study. It was also my responsibility to prevent any potential biased responses from the participants by selecting participants with no previous relationship with me. Also, I intended to conduct mock interviews if needed to test the interview guide and questions to uncover potential concerns and biases (see Kallio et al., 2016). I did not conduct any mock interviews.

I conducted this study to determine the strategies security managers used to prevent security breaches in SCADA systems' networks. My interest in SCADA systems' security has grown from working with the systems over the past 6 years. Although I do not provide direct SCADA security expertise to any organization, I have over 20 years' experience in the IT industry and more than 6 years working with SCADA systems. Kallio et al. (2016) discussed the role of researchers as the principal intermediary in data collection. The value and strength of the study result were influenced by incorporating and adhering to robust data collection. It is also imperative that qualitative researchers display skill and comprehensiveness during data analysis and interpretation (Leedy & Ormrod, 2015). Therefore, I used open-ended questions to evoke sufficient responses, open discussion, and answer follow-up questions from the potential participants. Additionally, I recorded the interview, took notes, and made observations during the interview process as part of my role as the researcher.

Adherence to the Belmont Report protocol provided by the U.S. Department of Health and Human Services is a vital component of research since it would ensure the integrity of the data and the conduct of the research in a manner that paid attention to the protection of participants and their rights. The use of the Belmont Report protocol and interview protocol, according to Heydon and Powell (2018), ensured the establishment of rapport and trust with participants. The Belmont Report protocol outlined a safe environment for the participants, respecting their autonomy and dignity and protecting their privacy. I emphasized to the potential participants that participation in the study was voluntary, and they can leave the interview any time they want. I conducted the interview process so that no harm would come to the participants by protecting their privacy. I will ensure I share my findings with them to benefit from the study, as the concept of justice in the Belmont Report dictates. Finally, I have completed the training course given by the National Institutes of Health (NIH), Protecting Human Research Participants (certification number: 2860239; see Appendix B).

I took adequate safeguards in this study to mitigate bias. According to Sprague et al. (2017), bias is introduced into a researcher by the researcher. I minimized the effect of bias by introducing safeguards, such as using interview protocol (see Appendix A) and member checking and avoiding injecting personal values, predispositions, and subjectivity. The semistructured interviews took place with the help of an interview protocol that facilitated conversations and enforced consistency in the interview questions. Member checking is an effective way of establishing rigor in qualitative research (Closs & Hadi, 2016). I used member checking to mitigate bias and to ensure the presence of rigor in the study. Finally, I recorded the interviews, transcribed the recorded interviews, and performed member checking to ensure the injection of personal values, predispositions, and subjectivity. Once I have used all the above safeguards, I avoided manipulating the collected data that may threaten the credibility of the research study.

Participants

The design approach for this study was the multiple case study, which according to Gunasekaran et al. (2018), relies on participants for its source of information and permits examination of a specific phenomenon in their original context. I selected the participants for my study from oil and gas organizations in the midstream sector in the Southwest region of the United States. According to Yin (2018), potential research participants should know about the phenomenon under study and provide suitable answers to the research questions. Therefore, I limited the participants to oil and gas organizations in the midstream sector located within the Southwest region of the United States having (a) SCADA security managers with at least 3 years of IT experience, (b) who have strategies for securing the SCADA systems, (c) at least 21 years of age, and (d) did not have a working relationship with me. The SCADA systems security manager is any individual involved in managing the SCADA systems' security, keeps track of security threats to the systems, regularly assesses the organization's vulnerabilities, and implements strategies to protect the SCADA systems from security breaches.

The process of recruiting the participants began as soon as I received institutional review board (IRB) approval. According to Maramwidze-Merrison (2016), potential participants may be identified by reviewing business listings and organizational databases, directly contacting participants, explaining to them the purpose of the research, and convincing potential participants of the importance of getting the research project complete through their participation. I recruited potential participants for this study by reviewing business listings on the internet and information gathered from professional colleagues. I contacted one of the executive leaders of each organization who served as the gatekeeper once I identified the organizations. I explained the research purpose and discussed the data collection process to ensure that I did not violate company policies. I asked the gatekeeper of the potential partner organizations to formally write a letter of cooperation to document their approval to participate in the study. I left the initial screening of the potential participants to the executive leadership of each organization to verify their qualifications and identify eligible participants. I obtained the contact information of the identified potential participants from the executive leadership. The next step was I invited the potential candidates through email, summarizing the purpose of the research study, the scope emphasizing the problem statement and the research question, and the informed consent form. I performed a personal screening of the participants to ensure they can participate in the study. I then discussed interview logistics such as date, time, and location once the participants meet eligibility criteria and they agreed to participate in the study. The provision of informed consent ensured participants' anonymity and protect their privacy (Roberts & Allen, 2015). I put other participants' needs into consideration to prevent confusion or surprises during the interview process. I also let the participants know that I would take notes, and the interview would be audio or videotaped.

Trust and working relationships would be built by first introducing myself and explaining the purpose of the study. According to Cheng et al. (2017), the establishment of trust will help to influence the quality and accuracy of the data. I further built on this connection through informal conversation focusing on their backgrounds, research topics and providing the interview questions in advance for review to clarify questions before the actual interview. Working with the participants to clarify any question they may have before the interview will help remove ambiguity and elicit genuine and detailed responses (Kallio et al., 2016).

Research Method and Design

In this research study, I explored the strategies security managers used to prevent security breaches in SCADA systems' networks. I chose a qualitative research methodology and a multiple case study design for this study. The use of qualitative research methodology provided me a deeper understanding of the phenomenon under study. The selected research methodology and design are in alignment with the research question. I collected research data from the selected oil and gas midstream companies in the Southwest region of the United States using semistructured, remote interviews via Zoom and Microsoft Teams. I also used organizational documents to understand the strategies security managers used to prevent security breaches in SCADA systems' networks.

Method

I used a qualitative case study method for the investigation. According to Almalki (2016), qualitative research allows researchers to draw detailed experiences from participants. I used the qualitative research approach to draw personal viewpoints and explore each participant's experiences. According to McCusker and Gunaydin (2015), questions about the *what*, *why,* or *how* are answered by qualitative research. I used a qualitative research approach to understand and explore *what* strategies SCADA security managers use to secure SCADA systems' networks to prevent security breaches. According to Almalki (2016), a qualitative research method is used to draw meaning from the different participants' experiences. The above statement applied to me since I extracted information and drew from the participants' experience about the strategies used for securing their SCADA systems. Also, Levitt et al. (2018) stated that the qualitative research method is suited for retrieving information from participants, especially when sharing their experiences using their own words. Since I collected data relevant to the study from the participants in their own words, a qualitative multiple case study was appropriate for this study.

The quantitative research method uses experimental methods, nonexperimental correlational designs, and quasi-experimental designs to explore the cause-and-effect relationship between variables such as skills, knowledge, attitudes, or abilities (King et al., 2019). I considered using a quantitative research method, but I did not select a quantitative method because researchers using quantitative methods emphasize mathematical or numerical. According to Boeren (2018), quantitative research methods use an objective and deductive process of inquiry to highlight generalizable statistical findings and test hypotheses. A quantitative approach is more suitable for explaining relationships between study variables through hypotheses testing and systematically comparing data. I did not test hypotheses or explore relationships in my study; therefore, the quantitative method was not appropriate for my research study. However, my research aims to gain an understanding of the phenomenon from the participants' experiences.

The mixed-method research methodology was considered but not selected despite its advantages over the other two methods. Mixed-method research, according to Kong et al. (2018), combined both qualitative and quantitative methods. A researcher may use the mixed-method approach to incorporate findings and draw conclusions from qualitative and quantitative components. According to Ivankova and Wingo (2018), the application of mixed-method research allows researchers to find answers to both confirmatory and exploratory problems within a single study to reveal a fuller picture of the problem. The mixed-method research was not deemed appropriate for this study due to the absence of numerical data and hypotheses testing. The use of mixed-methods research requires that the researcher have bits of knowledge of qualitative and quantitative techniques. It also requires a separate data collection process for the qualitative and quantitative aspects. The manipulation of both qualitative and quantitative methodologies is complex and may extend the completion time and effort, resource constraint, and increase the cost of the research. I did not select mixed-method research since I did not combine the components of qualitative and quantitative research in this study.

Research Design

I deemed the multiple case study research design appropriate to answer the research question for my study. According to Civitillo et al. (2019), the purpose of the multiple case study is to understand and describe a complex phenomenon in detail, especially in their real-world setting. Multiple case study design allows researchers to interview multiple separate groups and elicit data from their observations or experiences of the same phenomenon. Di Mauro et al. (2018) stated that multiple case study is ideal for identifying common patterns retrieved from historical details. Pieces of evidence retrieved from organizational documents, artifacts, observations, semi-structured interviews, and open-ended questions would help me gain insight into the strategies used by the participants to secure their SCADA systems. Also, case studies may be used, according to Jarvis and Williams (2017), when researching complex issues. Complex issues such as the strategies used by the SCADA security managers to secure SCADA systems' networks in their real-life settings are especially true since it involves collecting data from sources to depict and analyze the case. The case study also reflects the personal experiences of the participants. According to Fernández and Wagner (2016), a case study allows exploring the phenomenon in their natural context. Interviewing the participants regarding their experiences deploying strategies to secure the SCADA systems will allow me to acquire a holistic understanding of the problem under study. Case study design permits the experiences of those who are involved in a phenomenon to be studied (Ridder, 2017). Therefore, I chose the multiple case study for this study since it allowed me to understand the phenomenon under study in detail based on the participants' experiences.

Other research approaches to inquiry in a qualitative study apart from the case study may include phenomenological research and ethnographic research (Elkatawneh, 2016). The focus of ethnography design, according to Kaley et al. (2019), is on the culture or society under review, which often prompts a firm relationship between the participants and the ethnographers. Ethnography design was be appropriate for this research because the focus was not on society or culture. According to Trnka (2017), an ethnography study involves the researcher's immersion within the phenomenon under study. Since I was not immersed within the group under study, ethnography did not apply to this study. Ethnography design was not selected since my research question does not require exploring a society or a culture, nor was I to be immersed within the group under study. Instead, I sought understand the strategies used by SCADA security managers to secure SCADA systems' networks to prevent security breaches.

I also considered the phenomenological research approach for this study, but it was not selected. According to Alfakhri et al., 2018, researchers use phenomenological design when a phenomenon is to be interpreted from the participants' lived experiences and subjective viewpoint. The focus of this research study was not on human lived experience, so the phenomenological design was not selected. A phenomenological research design investigates human experiences through the lens of the people that lived through the phenomenon (Kruth, 2015). My research was not about how SCADA security managers experience the strategies they used, so the phenomenological approach is not applicable. According to van Manen (2017), the phenomenology approach may not necessarily expose the experiences recounted by the participants in detail. I sought to explore the detailed experiences of the participants in this study. The phenomenological research approach does not support collecting company documents (Marshall & Rossman, 2016). Apart from interviewing the participants to understand the phenomenon under study, organizational documents are also required to gain more insights from the organization's perspective.

Data saturation is essential in qualitative research because it helps to provide evidence of data validity. One of the challenges experienced by a researcher that uses the case study design is achieving data saturation. According to Lowe et al. (2018), data saturation is a point within the research where more data will not lead to a discovery of information about the research question. To accomplish saturation in this study, I collected organizational documents, correlated them with the participants' information, and further measured them against the compiled academic literature in the literature review section. Member checking is another means by which this study may attain saturation. Iivari (2018) stated that member checking allows participants or respondents to validate data or results of a study by checking to see if the results resonate with their experiences. I scheduled member checking interviews with the participants to ensure that they have no new information and confirmed my interpretation of their responses. I also ensured that I asked the same set of starting questions from the participants, followed by impromptu probing questions to understand the participants fully. Another method for achieving data saturation in a qualitative study, according to Hancock et al. (2016), is by tracking themes and subthemes for supplicates. To help track themes, I took notes during the interview and reviewed the collected data to ensure that I had no additional information. Once no new themes were presented from the interviews, this suggested that I had attained data and thematic saturation.

Population and Sampling

The population for this research study includes target organizations in the oil and gas organizations in the midstream sector, located in the Southwest region of the United

States. I ensured that the selection of the population for this study aligned with the purpose of the study, and I selected the participants from oil and gas organizations in the midstream sector within the Southwest region of the United States. Before they may participate in a research study, the researcher's specific characteristics must be specified and identified by the researcher (Nebeker et al., 2016). Furthermore, Asiamah et al. (2017) stated that the researcher must understand and describe the study's target population adequately. The organizations from whom I selected the participants have successfully implemented SCADA security management. The chosen individuals were full-time employees of the organization with a minimum of three years of IT experience securing the SCADA systems provided valuable information for the research. The participants were at least 21 years of age, and they do not have a working relationship with me.

I deployed the purposive expert sampling method based on selection criteria to distinguish eligible and qualified participants (Lucas, 2019). According to Cati et al. (2016), the research population must attain or meet a defined specified criterion. I, therefore, based the requirements for selecting the participants for the study on who best inform the research question. The researcher uses the purposive expert sampling method when there is a need to focus on the practitioners directly engaged in a specific research topic (Sarstedt et al., 2017). The adoption of the purposive sampling method based on preselected criteria was to ensure that the participants selected for this study meet the eligibility criteria to participate in the study. The executive leadership of each organization screened the potential participant to ensure they meet the eligibility criteria for selection. I adopted expert sampling, a subcategory of the purposive sampling technique, for this study. According to Lucas (2019), researchers use expert sampling when they seek relevant data from an experienced or known expert in the study area. Expert sampling allowed me to easily and quickly gather required information since I only contacted relevant and targeted participants.

The sample size used in qualitative research cannot be adequately determined by a specific rule but may be subject to saturation (van Rijnsoever, 2017). According to van Rijnsoever (2017), data collection and analysis should continue until a point when no new concepts emerge to determine the sampling size. Therefore, I evaluated potential participants based on the eligibility criteria and continued to recruit until I achieved sample size. Using a specific sample size is not required in a qualitative research method to yield ideal research results (Morse, 2015). Instead, the sample size in qualitative research depends on the goals of the research. Thomas (2017) asserted that the total population needed in qualitative research to reach data saturation is the driving principle for selecting an adequate sample size. Selecting adequate participants for qualitative research may be valuable to the research because the diverse opinions provided by the participants may result in invaluable information. When the sample is too large, according to Galvin (2015), it may result in redundant and unnecessary data. My sample size started with at least two participants from each organization, and I continue to recruit and interview qualified participants until I cannot observe new themes.

The key to any qualitative research is the interviews since they provide the primary means of data collection. The interview process should be made as comfortable as possible for the participants because hesitation from the participants may negatively impact data collection. According to Gagnon et al. (2015), detailed and rich information may be elicited from participants when the interview locations are familiar and comfortable. I conducted the interviews at an appropriate time and place agreed upon by the participants and myself. Therefore, the participants agreed to a safe and convenient location where there would be no distractions for the interviews. I also agreed with the participants about the preferred means to conduct the interview. I conducted the interviews through Zoom and Microsoft Teams. Skype is an effective method of eliciting genuine and detailed responses from participants (Sipes et al., 2019). It is crucial to establish trust and rapport with the participants before the commencement of the interview. The establishment of trust influences the quality and accuracy of the data collected (Cheng et al., 2017). I gained the participants' trust by introducing the research topic, discussing the scope of the research, and presenting them with the consent form to assure them I will protect their privacy. I also informed them that I would record the interview and take notes during the interview.

Ethical Research

Ethical considerations concerning the participants need to be made when conducting a research study. Walden University required that the IRB give its approval before data collection commences to ensure the appropriate conduct of investigators and the ethical treatment of participants. Ethical considerations, as stated by the Belmont report, according to Kowalski et al. (2017), include respect for individuals, beneficence, and justice. To ensure I followed due ethical considerations in this study, I first obtained the approval of the IRB before communicating with the potential participants. Once IRB has issued approval number 12-01-20-0731117 for this study, I sent the consent form to the participants through email. The participants indicated that they have read and agreed to the terms of the consent form, and they typed “I consent” in response to the email containing the informed consent form. According to Roberts and Allen (2015), informed consent ensures the anonymity of the participants and protects their privacy. The consent form includes information about the study to include ethical considerations, the right to withdraw from the study at any time for any reason and without notice, voluntary participation in the study, dangers that may exist, and participants' intent to participate. Furthermore, the consent form indicated the absence of incentives, financial or otherwise, for the participants. Lastly, the informed consent form also includes potential benefits, my contact information, and that of Walden Research Participant Advocate, actions that I will take to ensure participants' anonymity and privacy.

Participants may decide to withdraw from the study at any point in time if they decide to stop participating in the study. Participants in a study have the right to make decisions to participate in a study or not (Williams & Anderson, 2018). I provided the terms and conditions for participating in the study to the participants in the consent form. I ensured that the participants were aware of their rights to opt-out of the study whenever they desire to do so. The participants were also made aware that participation in the study is voluntary. Beneficence and justice involve providing benefits to participants in a study and minimizing risk (Laage et al., 2017). I ensured not to expose the participants to any risk that is more than they will typically encounter during the routine execution of their daily duties. Offering incentives to participants to participate in a study may assist in attracting participants. However, it may also lead to participants remaining in a study against their will because of the incentives provided (Lee et al., 2015). Offering incentives may also elicit biased responses from the participants whose interest is what they get out of the study. I informed the participants that I will provide no incentives and monetary benefits. Apart from explicitly defining the purpose of the study, how the information provided would be safeguarded, procedures for opting out of the study, this study will provide the participants with the conclusions, information, and opinions gathered. This study will also provide the participants insights into the strategies security managers used to prevent security breaches in SCADA systems' networks.

The relevant documents in this study, such as the collected data, organizational documents, audio-recorded interviews, and transcriptions, would be protected to ensure privacy and confidentiality. According to Dempsey et al. (2016), participants' anonymity should be guaranteed in a study by the researcher so that any data presented are not traceable to them. The actual names of the participants and their organizations were protected using code names. I have stored their actual names and the associated code names in an encrypted spreadsheet. All the information gathered was classified into two viz: (a) Electronic information include password-protected files stored in an encrypted external drive. (b) The hard copy or print form I have locked up in a safe fireproof storage cabinet. Both electronic and hard copy documents obtained during the data collection process would be kept securely for five years from the final research approval date. I will delete the electronic records after five years, while the hard copy documents would be shredded. According to Singhal and Bhola (2017), researchers must protect the confidentiality of the information provided by the participants to ensure ethical research practices. After five years, permanently deleting the data would ensure compliance with ethical practices and protect the study participants' privacy.

Data Collection

Instruments

The researcher is the primary instrument for collecting data in a qualitative multiple case study. As a researcher, I recognize myself as the primary data collection instrument. According to Yates and Leggett (2016), the researcher must work directly with the data in a qualitative study as the primary data collection instrument. Semi-structured interviews and a review of organizational documents were the primary data collection tools for this study. I used semi-structured interview questions to collect information from the research participants. During the semi-structured interviews, participants provided answers to open-ended questions to elicit their viewpoints on the research topic. According to Nebeker et al. (2016), semi-structured interviews are used to gain insights into the participant's experiences and encourage extensive feedback using open-ended questions. Semi-structured interviews allow interviewees to reflect on their personal experiences (Boyacı, & Guner, 2018). The participants reflected on their own experiences when they provided answers to the open-ended questions. My focus was to use semi-structured interviews based on the interview questions identified in (Appendix A) to explore the strategies security managers used to prevent security breaches in

SCADA systems' networks. Once I finished collecting the data, the next step was I organized and analyzed the data to answer the research question.

The created interview protocol (see Appendix A) served as a guide before, during, and after the data collection process. According to Dikko (2016), interview protocol serves as guidelines or a set of rules for conducting interviews. Probing questions may also be asked due to the semi-structured nature of the interview to gain insight into the research topic. The open-ended questions in the interview allowed the participants to evaluate the research question and provide elaborated responses. I conducted the interviews after work and through Zoom and Microsoft Teams to increase the reliability of the study. Renz et al. (2018) observed extensive interviews, audio recordings, and note-taking during data collection in qualitative research. I, therefore, ensured that I took notes during the interview and, with the permission of the participants already documented in the informed consent form, audio-recorded the interviews. Audio recordings are used in a research study to verify the accuracy of the transcriptions during the data analysis stage (Simpson & Quigley, 2016). Note-taking and audio recording of the interview ensured a complete record of the interviews for analysis. I identified the participants in the notes and recordings by code names to protect their privacy. The purpose of taking notes and audio recording the interview was to ensure accuracy when analyzing and presenting findings from the collected data.

According to Yin (2018), documentation could be used to verify further the data collected from the interviews. I also reviewed organizational documents such as security policies, access controls, instructional manuals, and training materials. According to

Baxter et al. (2016), reviewing and analyzing organizational documents will assist in gaining a deeper understanding of the strategies used by the SCADA systems' security managers. The secondary data source was the organizational documents, which I used to verify findings from the original data collected from the interviews. The reviewed documents assisted in identifying core elements, recurring themes, and patterns used by security managers to prevent security breaches in SCADA systems' networks.

After completing the interviews and reviewing the organizational documents, I performed member checking to ensure credibility. Member checking followed to ensure the accuracy and reliability of the data and that the analysis contained detailed participants' perceptions (Birt et al., 2016). According to Iivari (2018), member checking involves offering research results to participants to scrutinize and validate. I used Otter.ai, an open-source tool, to create a transcript of the recording. I reviewed the transcripts multiple times to create a bulleted list summarizing key points of the targeted participant's response. I then conducted a follow-up interview for member checking where I provided the summary of the participant's response for correction, validation, or to expand on the interpretations. Also, I asked follow-up questions during the interview to clarify the participant's responses. According to Dikko (2016), the data collection instruments used in any research study must pass the reliability and validity test.

Data Collection Technique

In a qualitative multiple case study, the data collection technique includes open-ended interviews, reviewing organizational documents, and archival records. The main instrument in the data collection process is the researcher (Clark & Veale, 2018).

Interviews are one way researchers can use to collect data and uncover additional information in qualitative research. I paid close attention to all assumptions that may prevent the study's objective from being achieved as the main instrument in this research study. Such assumptions include properly screening the participants, ensuring the participants sign the consent forms, putting the participants' needs into consideration to avoid confusion, and letting the participants know that I will take notes. The interview was audio recorded. I conducted interviews for this qualitative study using the interview protocol in Appendix A. I explained the purpose of the interview and the investigation to the participants to ensure they understand the purpose of the study. I paid close attention to the participants' physical, verbal, and non-verbal behavior in the natural setting and took notes and recorded the interview. I took notes not to disrupt the interview process, and the notes served as a second instrument. I prompted the interviewee to expatiate more if they provided a short answer to a question. Kallio et al. (2016) opined that researchers could modify the interview questions in a semi-structured interview based on the responses given by the participants. I adjusted the interview protocol depending on the answers provided by the interviewee to ask further probing questions to obtain more responses.

The second data collection technique that I used in this qualitative research was to review organizational documents. Yin (2018) stated that the use of documentation further verifies the data collected from qualitative interviews. The documentation technique in this study involved the following five steps: (a) accessing the documents, (b) confirm their authenticity, (c) study and understand the materials, (d) conduct data analysis, and

(e) make use of the data. The purpose of using the documentation technique is to complement the qualitative interviews. The strength of one method complements the weakness of the other method when the two methods are combined. According to Palinkas et al. (2015), multiple sources sums up evidence that will support the explanation of a phenomenon under study in qualitative research. The organizational documents provided more details to the explanations given by the interviewees. According to Baxter et al. (2016), reviewing organizational documents would allow researchers to understand security strategies in critical infrastructure. I asked the respective interviewees to identify and provide access to relevant organizational documents such as strategies, policies, operating procedures, access controls, educational materials, emails and the internet, and working aids. Organizational documents with credible sources are necessary to identify a robust dataset consistent with data analysis, participant interviews, and triangulation (Tas et al., 2017). The organizational documents helped identify core elements, recurring themes, and patterns used by security managers to prevent security breaches in SCADA systems' networks.

The researcher must consider the advantages and disadvantages of data collection techniques used in a qualitative study. Two forms of data collection techniques were used in this study, as mentioned above. The data collection techniques were semi-structured interviews and the review of organizational documents. According to Nebeker et al. (2016), one of the advantages of using semi-structured interviews is to gain insight into the interviewee's experiences and encourage extensive feedback by asking open-ended questions. I asked additional questions during the interview, which benefited the study to uncover new data. It also allows for further probing to seek clarification for unclear information. Semi-structured interviews provide means of capturing non-verbal cues, enhancing data collection during an interview (Jamison et al., 2018). The non-verbal cues could be hesitation or pause in a speech, allowing the researcher to chip in a new question or pursue additional questioning lines, which may enrich data collection. Another advantage is that a semi-structured interview provides an opportunity to meet with the interviewees face-to-face to ask them questions about the research topic.

There are also disadvantages to using the semi-structured interview as a form of data collection technique. One such disadvantage is the introduction of bias by the researcher. According to Sprague et al. (2017), researchers may introduce bias into a research study. The researcher's introduction of bias into a research study may result in misrepresentation of the collected data, which may eventually skew the study results. It is, therefore, imperative that the interviewees are allowed to verify and ensure the accuracy of the collected data during member checking. The use of interview protocol with every participant will ensure the removal of bias. Another disadvantage is that planning, coordinating, and choosing a neutral location for the interview requires considering each participant. According to Rimando et al. (2015), selecting a favorable and neutral interview location free from distraction is of paramount importance to conducive data collection. The environment must be conducive for conducting interviews, free from background noise and distractions not to impact that interpretation.

I used member checking in this study to ensure the reliability and validity of the data collection instruments. According to Connelly (2016), Member checking can be used to establish the credibility of data through extended engagement and triangulation. According to Varpio et al. (2017), triangulation involves analyzing the various data collected from numerous perspectives. Triangulation was used in this study to align all the information collected through the various interviews, organizational documents, and member checking. Member checking is used for exploring and validating the credibility of the data collected during the interview (Birt et al., 2016). After the initial interview, member checking was done to review my interpretation of the collected data for accuracy. I scheduled member checking interviews with the participants to review and validate the interpretation of the data collected. I repeated this process until the participants confirmed that I accurately reflect their experiences in my analysis. Member checking also helped ensure that conclusions reached reflects the participants' intended meaning. Finally, I will ensure that the study's final report goes back to the participants to verify the accuracy of the themes.

Data Organization Techniques

The information and evidence collected during a qualitative case study are significant, thereby necessitating proper organization and handling. Some of the documents include emails, consent forms, audio recordings, organizational documents, and transcripts of the recordings. According to Lasrado and Uzbeck (2017), researchers can employ different data handling and organization methods to track and manage their research data. I used different data organization techniques such as researcher notes, researcher logs, reflective journals, and file naming in this study. Researchers use logs and journals to record their thoughts, experiences, and insights during research study and provide materials to review for identified concerns during the research phase (Orange, 2016). I maintained notes, journals, and logs during the data collection phase because they are vital resources for following up on ideas to reveal new themes. I kept a log for each participant to help document ideas and thoughts that can clarify points or follow up on a question. I used the logs to minimize bias, identify challenges, provide an audit trail, and document emerging themes and patterns. I also used a reflective journal to document all my activities and experiences during the interview process. According to Cuellar (2018) and David and Hitchcock (2018), a reflective journal summarizes and tracks the researcher's experiences during a research study. The reflective journal may also serve as an additional data resource to reflect on after the research process.

I transcribed the audio recordings into a format that is human-readable and accessible such as Microsoft Word. I concealed the Identities of participants and their organizations using codes such as O1, O2 for Organization 1 and Organization 2, P1, and P2 for Participant 1 and Participant 2. According to Gergen et al. (2015), personal information such as organizations' identities, participants’ names, and employment positions is best protected with codes. I used the above naming convention to store the transcribed audio recordings of the different interviews to protect the real identity of the participants. I created folders using the naming convention above to categorize documents according to participants and their organizations for easy retrieval.

All documents such as emails, consent forms, organizational documents, and transcripts of the recordings are encrypted and stored in personal cloud storage, Microsoft OneDrive, to ensure the data will not be lost. Protecting the confidentiality of the information provided by the participants in a research study will ensure ethical research practices (Singhal & Bhola, 2017). I backed up all the documents in password-protected files and stored them in an encrypted external drive. I encrypted the documents to guarantee the confidentiality of the participants. I labeled and categorized the hard copies of the documents, such as the notes, logs, and organizational documents, using the naming convention mentioned above and stored them in a locked file cabinet in my home. I will keep all the documents, both the electronic and hard copies, for five years in a secured location, and destruction and disposal will occur at the end of the five years. I will permanently delete the electronic copies of the document while I will personally shred the hard copy documents.

Data Analysis Technique

Collecting, organizing, analyzing, and interpreting data in qualitative research is essential since open-ended questions are asked to discover meaning. According to Johnson et al. (2017), data analysis is a crucial and complex phase in a qualitative research study. The data analysis phase involves examining textual data collected from interviews and organizational documents and organizing and converging them into themes that support my research questions. I categorized the textual data collected from the interviews and the organizational documents to explain my research topic. My focus during data analysis was to analyze the strategies security managers used to prevent security breaches in SCADA systems' networks. I used methodological triangulation in this study to validate the findings from the various data collection sources. According to Joslin and Muller (2016), triangulation assists the researcher in overcoming weaknesses that may exist in the data with the combination of multiple data sources in a research study. Since I collected the data from multiple sources, I used methodological triangulation to enhance the validity and reliability of the study. I used methodological triangulation to align the information collected from the various sources, such as the semi-structured interviews, organizational documents, and the researcher's notes. According to Cai et al. (2015), Dube and Uys (2015), triangulation ensures the validity and reliability of a research study. Methodological triangulation will add more decisive confirmation and strengthen the understanding of the research topic.

The primary purpose of the analysis phase was to uncover the key concepts from the collected data. According to Johnson et al. (2017), the strategy for data analysis involves data compilation, disassembling data, reassembling data, interpreting data, and making conclusions of the data through recursive relationships. I organized the data collected during the interview phase and the reviewed documents using the code names associated with the participants. I transcribed the recorded interviews into textual form and compared the different interview responses. I constructed themes from the transcribed data once the collected data had been disassembled and reassembled. As observed by some researchers, the results of a research study need to be organized by themes to ensure the answers given by the participants are correct (Low et al., 2016; Ranney et al., 2015; Sutton & Austin, 2015). I tracked themes to identify similarities, analyze patterns, concepts, and group responses similar to understandable categories using NVivo 12. I adequately reviewed data to gain familiarity to generate codes that reflect the research question.

I also used field notes, which served as a complementary data source to document ideas during the analysis phase. I applied coding to explore associations in the data and to identify patterns against the collected data. The use of NVivo software helped to organize and analyze the unstructured data collected from the interviews. The fundamental task is to select the themes during the analysis phase (Emmel, 2015). The researcher may use the following steps according to Emmel (2015) in selecting themes: (a) emphasize commonly used words, (b) reduce the themes, (c) rank the themes, (d) and associate the themes with the conceptual framework and the research question. The discovered themes were then further analyzed and linked to the literature review and the conceptual framework.

Member checking provides the participants with the opportunity to review the interpretation of their responses and provide feedback (Stillwell et al., 2018). I loaded the documents into NVivo only after the participants re-examine my interpretation of the responses and make necessary adjustments based on the participants' feedback. According to Maher et al. (2018), NVivo enables researchers to code and organize themes. The NVivo software alone cannot by itself perform all the necessary work of coding and organizing themes. The researcher must label, sort, code, categorize, and compare the collected data. NVivo software will promote analytical flexibility and improve the transparency and trustworthiness of the research process (Kaefer et al., 2015). I broke down the collected data into categories and assembled them based on similar themes. Interpretation and conclusion were drawn from the assembled data once I have ensured the themes aligned with the conceptual framework of GST and the literature review on the strategies security managers used to prevent security breaches in SCADA systems' networks.

The last phase of the data analysis process was the generation of reports. The reports consisted of significant themes tied back to the literature review and the conceptual framework. GST was the conceptual framework that serves as the lens used to explore the strategies used by SCADA security managers to secure SCADA systems' networks to prevent security breaches. NVivo software played an essential role in sorting out the themes in the final report generation.

Reliability and Validity

The findings of a research study should have elements of authenticity. The research study must be reliable and valid to ensure authenticity. Reliability of a study stem from the fact that the study must have the same outcome if repeated in the same manner (Leung, 2015). While validity, on the other hand, is the extent to which an instrument is measured (Marshall & Rossman, 2016). Reliability and validity are techniques used in a research study to minimize bias and ensure transparency. According to Morse (2015), the quality and trustworthiness of a research study may be measured using the following four criteria: dependability, credibility, transferability, and confirmability. Various techniques may be used to ensure validity and reliability, such as member checking, reviewing the interview transcript, and triangulation.

Dependability

In qualitative research, dependability refers to the consistency and reliability of the findings of a study and its ability to produce the same results when repeated in the same manner (Amankwaa, 2016). Other researchers should be able to understand how the findings of the research were derived if the study is dependable. According to Crowe et al. (2015), other researchers can follow the trail of decisions in dependable research. Various methods, such as member checking, interview protocol, transcript review, may improve dependability in a study. Dependability was achieved in this study using member checking and audit trails of procedures and methods used in the study. Member checking allows the study participants to directly confirm the study results (Wu et al., 2017). Member checking as a quality control ensures that the results of a study are accurate, credible, and valid (Nelson, 2016). The participants had the opportunity to review the data collected during member checking for accuracy and ensure it resonates with their experiences. Another method I used to ensure dependability was to provide the audit trail of the procedures and methods used in the study. According to Mandal (2018), the audit trail may be facilitated through proper documentation and a detailed explanation of data collection and analysis processes. I ensured that I properly document all procedures during the research study by using a reflexive journal and research log to document my process so that a reviewer or reader may understand how the study's findings were derived.

Credibility

Credibility is vital to achieving validity since it involves ensuring the study's credibility from the participants' perspective in the research. According to Allred et al. (2017), credibility involves allowing participants the opportunity to correct misinterpretations or errors in research findings to the context of the study. Member checking is one of the methods that can be used to increase the credibility of a study. In a qualitative study, member checking establishes rigor (Closs & Hadi, 2016). I used member checking in this qualitative research to confirm my interpretation of the participants' views. I scheduled member checking interviews with the participants to confirm that they have no new information to offer and confirm if the results resonate with their experiences. According to Iivari (2018), member checking allows participants to validate the results of a study by ensuring it was the correct interpretation of their experiences. Member checking will make the study credible from the participants' perspectives because the participants verified the collected data for accuracy and credibility.

I used methodological triangulation as another method in this study to ensure credibility. Since the source of data was from multiple sources such as semi-structured interviews, organizational documents, and the researcher's notes, it is imperative to use triangulation to align all the information collected from various sources. According to Joslin and Muller (2016), weaknesses in a data source when multiple sources are involved are overcome using triangulation. I compared the different interpretations from the various interviewee to identify similarities and differences between the data sources and themes. I also deployed methodological triangulation in this research to obtain supporting evidence from the semi-structured interviews, organizational documents, and the researcher's notes to ensure that the data collected from the various sources answer the research question.

Transferability

In qualitative research, an essential aspect of reliability is transferability. According to Allred et al. (2017), transferability involves comparing research findings to findings of similar studies to determine commonality. Researchers must ensure they provide enough information to ensure other researchers can apply the study's results to different situations. I ensured that the methods and procedures were documented and thoroughly described the assumptions and research context. Weis and Willems (2017) noted that techniques that will allow for the transferability of results beyond the specific study must be applied. One such technique of ensuring transferability includes retaining the interview protocol, organizational documents, results from the study, and other documents used in the research study for five years. Should there be a need to reuse the artifacts, the artifacts retained for five years would provide data for further analysis. Also, Connelly (2016) stated that transferability is enhanced when researchers are transparent about data analysis and trustworthiness and provide accurate descriptions and rich content. I ensured that I adequately document the data collection process, analysis, transcript review, member checking process, and triangulation.

Confirmability

Confirmability in qualitative research ensures that the research results can be collaborated or confirmed by other researchers. Confirmability is the level at which the findings of a research study represent the participants' feedback and the participants' input (Korstjens & Moser, 2018). Furthermore, Arundell et al. (2018) stated that confirmability occurs when the results of a study reflect the responses given by the participants without any bias from the researcher. I minimized bias and ensured that the participants' responses were confirmable using the interview protocol in this research study. Interview protocol serves as a set of rules used for conducting interviews (Dikko, 2016). The interview protocol (see Appendix A) served as a guide before, during, and after the data collection process. I used methodological triangulation to compare the findings from the semi-structured interviews with organizational documents and the researcher's notes. According to Ridder (2017), the data collection process leverages triangulation to combine interviews, documents, and observations. I used methodological triangulation to authenticate the accuracy and quality of the research findings. Peticca-Harris et al. (2016) emphasized the use of a researcher log and reflective journal to ensure the organization of data and opportunity by the researcher to identify patterns and themes in the data

Transition and Summary

Section 2 of this study restated the study's primary purpose, describing my role as the researcher regarding data collection, how I selected participants, research method and design, population and sampling, and ethical considerations. This section's other key points include the data collection process, such as the data collection instruments, data organization techniques, and data analysis techniques. I also discussed ensuring the reliability, validity, dependability, credibility, transferability, and confirmability of this study.

Section 3 of this study consisted of a brief introduction of the study's purpose, followed by presenting findings from the collected data. Section 3 also includes a detailed discussion on how the results of this research will apply to IT's professional practice and how it could affect society. Finally, section 3 also includes recommendations for action and a further research study to improve practice in the IT field and the reflections and conclusion of the research study.

Section 3: Application to Professional Practice and Implications for Change

In this study, I aimed to explore the strategies security managers used to secure the SCAD systems' networks to prevent security breaches. In this section, I presented my findings from the analyzed data. Also, I described its application to professional practice, the implication for social change, a recommendation for action, and further research. I concluded the section with my reflection and study conclusion.

Overview of Study

This qualitative multiple case study explored the strategies security managers used to prevent security breaches in SCADA systems' networks. The data came from oil and gas midstream companies located in the Southwest region of the United States. I collected the research data through semistructured interviews, organizational documents, field notes, and reflective journals. The findings showed the methods used by SCADA security managers to secure SCADA systems' networks to prevent security breaches.

The four major themes revealed during the qualitative multiple case study are (a) the importance of security awareness and workforce security training, (b) the use of technical control mechanism, (c) establishment of standard security policies, and (d) the use of access and identity management techniques. The four major themes aligned with the literature review and the study's results tied back to GST, the conceptual framework. I explored and described the four major themes in the next section.

Presentation of the Findings

The study's overall research question was "What strategies do SCADA security managers use to secure SCADA systems' networks to prevent security breaches?" I described and explored in this section each of the four major themes revealed from this study. The strategy I used for responding to this research question involved conducting semistructured interviews with six middle-level managers from three organizations located in the Southwest region of the United States. As I conducted the semistructured interviews, my goal was to understand the different strategies used to secure SCADA systems' networks to prevent security breaches. I entered the six participant's transcripts and other relevant documents into the NVivo 12 software for analysis and subsequent identification of four major themes. Nvivo software enables researchers to code and organizes patterns or themes (Maher et al., 2018). All the participants in this study are qualified to participate since they had a minimum of 3 years of experience securing and working with the SCADA systems. The organizations had codes O1, O2, and O3, while the respective participants had codes P1, P2, P3, P4, P5, and P6. I used O1D1, O2D3, O3D4 to represent Organization 1 Document 1, Organization 2 Document 3, and Organization 3 Document 4. The main intention of using codes was to protect the participants' privacy, their organizations and uphold high-level confidentiality. All the participants duly signed the informed consent form by typing “I consent” in response to the email containing the informed consent form to express their willingness to participate in the study.

I used methodological triangulation to validate the data collected during the semistructured interviews, publicly accessible documents from each organization, and notes. I used Otter.ai, an online transcribing software, to transcribe the audio-recorded interviews. I loaded the transcriptions, organizational documents, and observations from the interviews into Nvivo 12 software for in-depth data analysis. The following four main themes emerged out of my analysis: (a) the importance of security awareness and workforce security training, (b) the use of technical control mechanism, (c) establishment of standard security policies, and (d) the use of access and identity management techniques. I illustrate the four major themes in Table 2 below. I covered all the four major themes in the analysis below, linking them to the literature review, other scholarly studies, effective IT practices, and GST, the adopted conceptual framework in this study.

Table 2

Major themes from Data collection

Major themes	Participant		Document	
	Count	References	Count	References
Security and awareness training	5	50	6	12
Technical control	6	64	7	10
Security Policies	5	48	7	10
Access/Identity Management	6	44	6	8

Theme 1: Security Training and Security Awareness

Overview

The first theme that emerged during the research data analysis stage was security training and security awareness. Information security training, education, and awareness of security risks are essential to providing employees with the required knowledge and skills to comply with security policies and protect organizations from cyberattacks

(Alshaikh et al., 2021). Security managers in most organizations use security training and awareness programs to improve employee security behavior towards positive cybersecurity objectives. According to Hart et al. (2020), cyberattacks increase sophistication and number, causing organizations to invest in professional training courses to raise their employees' awareness of cybersecurity attacks. Organizations need to develop robust security training and awareness programs to protect their information assets. Table 3 below depicts the number of references related to security training and security awareness theme and subthemes.

Table 3

References to Security Training and Security Awareness

Major themes	Participant		Document	
	Count	References	Count	References
Personnel Security Training	5	50	6	12

Findings from Participant Interviews

One of the significant subthemes that emerged during the analysis stage was security awareness training. Most of the respondents felt that employees should have security awareness training to sensitize them to the high-security risk associated with the industry. The first line of defense against cyberthreats is creating awareness and getting ready through cybersecurity training. The study's findings support creating a security awareness program to make the employees conscious of the security risks and the potential consequences. P2 stated that "a function of having people being aware of security and taking action to make sure that it doesn't happen" had been the reason for the very few data breaches into operational SCADA networks. Likewise, P6 observed that "the biggest one is just training, in terms of making you aware of the risks and potential scenarios, and of course, the liability that it could cause." P3 mentioned some of the liabilities in the following statement "When you're talking about a SCADA system, possibility for physical harm or even death is a possibility from a malicious actor. So, with that in mind, vendors and customers have a very high-security awareness in their organizations." Organizations are facing substantial threats from malicious actors, such as phishing attacks or social engineering attacks. As a result, organizations become aware of the importance of training their employees to become the first line of defense for their organizations.

The participants mentioned new threats coming up constantly. According to P2,

> New phishing scams come out all the time, and they can look official like the one I was seeing on the TV just the other day. And it's a perfect example. It starts with an offer that looks official from some government department. An offer, I think the way it was phrased, is something about a stimulus, not stimulus fund, or stimulus refunds, or anything like that. But it was you're entitled to stimulus money or something along that lines, and it's got what appeared to be legitimate departmental logos, watermarks on the paper. And it goes as far as giving you fake certification documents from the various supposed ID certifiers that this is a real thing. Okay. It looks official. It looks like something that would come from a

> government, the US government in particular. Yes. Well, it's very hard to train everybody to be completely aware of those all the time.

P1 stated that employees need “understanding about not giving out your passwords, not getting phishing emails, or getting viruses unintentionally on your computer and bringing it into the SCADA system.” P2 buttressed the point with an example stating that:

> It takes one person in a moment of vulnerability to crack into a system. I'll give you a personal example, people. And this happened to me quite a number of years ago, just when I had come down to the US from Canada. And I got nicely set up with credit cards and the social security number and all that all of the stuff that I needed. Well, I got a text message from what appeared to be my bank saying something about my account had been compromised, or frozen, or something like that. And please call, you know, please call this number. So, I did. I was in a moment of panic then; I wasn't thinking clearly. Okay, and that moment of panic. Unfortunately, nothing ever seriously happened about it. I think the worst thing that happened was I had to get my debit card replaced.

P3 reiterated that,

> At least with all of the latest SCADA implementations, it's been my experience that security is usually the first highest priority issue for most SCADA teams now because it's cheaper to spend our money than to allow the system to be breached. Yeah, I think it has to do with one being there's a lot more awareness in the industry.

One of the participants mentioned ongoing cybersecurity awareness training to sensitize employees. P4 explained,

> Security training at my company, we're going through it right now with a set of Cybersecurity awareness training sessions. So, making people aware of how sensitive this stuff is and how it can get divulged is important, teaching people to use strong passwords, teaching people to or enforcing that people update their passwords regularly. That's another big thing. Don't use the same password for all your accounts; something simple like that. So that's all part of education and awareness training.

Organizations are exposed to various threats to their information assets despite having advanced technological systems and policies in place due to human error. Human error exposes organizations to cyberattacks without adequate training. Therefore, cybersecurity training for employees is crucial since they are the first line of defense for their organization.

Organizational Documentation Support

Six of the organizational documents used for methodological triangulation emphasized the importance of the first theme. The authors of O1D2 stated that security threats to pipeline operations could disrupt service and significantly impact the environment, public health, and the economy. The organization, therefore, employs cybersecurity programs and physical security measures to deter, prevent, and mitigate the threats. Evidence from the authors of O2D1 agreed that vulnerabilities lie in systems and people. The authors of the organizational document went further to say that decreasing vulnerability risks requires a never-ending vigilant stand. The authors of O2D1 reiterates that the organization takes numerous measures such as a layered security approach, consistent training, audits, and testing to mitigate cyberattacks' risk.

Evidence from authors of O3D1 indicated that cyber risks are unique and are constantly changing. The organization thereby aligned its cybersecurity program with the National Institute of Standards and Technology Cybersecurity Framework. The authors of O3D1 stated that some of the critical programs designed to mitigate against cyberattacks include risk assessments conducted throughout the year and numerous cybersecurity training and awareness programs for employees, and tests of incident response plans. Further evidence from the O2D2 stated the importance of receiving training from partner organizations like the Federal Bureau of Investigation (FBI). According to the authors of O2D2, an FBI agent simulated a phishing attack through what looked like a legitimate email. The FBI agent emphasized that the hackers are clever and would attempt to get through any employees.

Other evidence emerged from Partner Organization 2 through its document O2D6 evaluated threats due to the Covid-19 pandemic. Most employees work remotely from home due to the covid-19 pandemic. The authors of O2D6 emphasized providing a security awareness and training program revolving around remote work risks. According to the authors of, organizations must collaborate with Enterprise Information Technology (EIT) to secure new remote work solutions.

Connections to the Conceptual Framework and Other Scholarly Studies

The conceptual framework adopted for this study is GST. GST stems from the concept that a system is a combination of parts that form a complex whole (Rapp et al., 2020). One of the essential principles of GST is holism. According to Johnson (2019), holism is a characteristic of systems working together to interact collectively with their environment. Simola (2018) stated that GST is a robust framework used to understand organizations' entirety when all the organizations' components work together to accomplish their objectives. Barca (2017) emphasized in alignment with the holism concept of GST that any information security system that fails to function in totality will result in a breakdown of its defenses. Protecting organizational information assets against cyberattacks helps to achieve a foundation that is part of GST. Through security awareness and workforce security training, organizations have proactively implemented the GST principle of protecting their systems against cyberattacks.

Evidence gathered from the study findings acknowledged employees' security awareness and training as essential in securing the SCADA systems. Ani et al. (2019) stated that technology is weak and vulnerable as the people who developed and operated it and the processes designed to use it. The interaction between vendors, organizational partners, active employees, and end users generally shaped the presence of an organization in cyberspace (Sallos et al., 2019). Employees are part of the whole security apparatus, and a complete analysis of this aspect only without reference to the entire security system will lead to a security disaster. According to Abou el Kalam (2021), the SCADA systems do not receive adequate protection from several attack vectors despite their importance, leading to economic and human damage. To deal with the different attack vectors threatening the confidentiality of sensitive information in the SCADA systems' networks, we need to consider all aspects of the system and not a few sections.

GST embraces principles that focus on the interdependent subsystems working together in a complex system. GST demonstrates the impact of interdependent components such as technology, processes, and people who worked together to protect organizational assets instead of subsystems working in isolation to achieve the same objective (Simola, 2018). Modified system components without taking the system components' entirety into considerations may lead to the system's destruction (Van Assche et al., 2019). Information security should be holistically considered and not by its parts. The study agrees with the concept that systems security is only valuable when we look at the whole package as against individual items.

Other scholarly studies also align with employees' security awareness and security training uncovered during the data analysis stage. The end users, in this case, the employees of an organization, hold a vital role in securing the information assets of any organization since they are the weakest link in the information security chain (see Dang-Pham et al., 2017). Employees play a significant role in information security, and we cannot isolate them from the whole system. Grassegger and Nedbal (2021) confirmed information security awareness and training as central factors for information security. Employees can resist security vectors such as social engineering due to information security awareness and training. Security training and awareness are vital to prevent the misuse of information systems. According to Gratian et al. (2018), security awareness and training are necessary to resolve data breaches due to human error.

Despite the implementation of security awareness and training in many organizations, the rate of unintended security breaches is on the increase. According to Alshaikh et al. (2021), employees caused 70% of security incidents because they did not comply with organizational information security directives. Hackers know that the employees provide a soft attack surface that they can successfully exploit. Therefore, organizations should approach employee security awareness training as a critical ongoing process in a more extensive security awareness program. According to Kim et al. (2020), security awareness training through ongoing organizational efforts has a deterrent effect and reinforces acceptable usage guidelines. The findings from the study participants and the scholarly literature are in alignment since both agreed that the adoption of security awareness and training programs influences employees' information security compliance.

Reference to Effective Information Technology Practice

All six participants emphasized the role of information security awareness and security training in sensitizing employees to the security risks and threats inherent in the SCADA systems' networks. Also, five of the organizational documents reviewed supported this statement. The SCADA systems' networks, if compromised, may result in the loss or degradation of services such as electricity, water utilities, health care, and oil and gas distribution. All the participants, supported by the five organizational documents, pointed out the need for employees' security awareness and training. According to Yamin et al. (2020), cybersecurity training can be of two forms: (a) for security professionals and (b) for no-professionals. Security training for professionals aims to improve their understanding of the latest threats and improve their skill levels towards mitigating against them. At the same time, security training for nonsecurity professionals is to increase their cybersecurity awareness.

The purpose of security awareness training is to equip employees with the knowledge they require to deal with cyber threats (He et al., 2020). Security awareness training should be a critical ongoing practice rather than a one-time event. According to Goh (2020), organizations must (a) train and educate all stakeholders irrespective of their role since every person plays an essential part in protecting organizational assets, (b) conduct an internal cybersecurity audit to measure progress and evaluate knowledge gaps across the organization, and (c) lead by example by ensuring all managers across departments and executives participate in cybersecurity training courses. Security is everyone’s responsibility because harmless behaviors can have enormous consequences. The lack of awareness and formal security training by users determines the success of cyberattacks (Chowdhury & Gkioulos, 2021).

Employees can rectify unsafe and suspicious practices and avoid being vectors of software attacks through security awareness training (Maiorca et al., 2020). Proper cybersecurity training will allow employees to recognize the threats to their organizations and take the right actions to reduce its risks. According to He and Zhang (2019), cybersecurity training that is adaptive, interactive, and incorporates on-the-job training is usually very successful. Since cybercriminals capitalize on human weakness, the adoption of robust employee security awareness training should be encouraged.

Zuopeng et al. (2021) stated that security awareness training programs fall short because the focus of the training is misaligned.

The use of a feedback mechanism is vital in measuring the effectiveness of security awareness training. Surveys, user logs, and other network metrics are used in measuring the effectiveness of the security awareness and training program (Choi et al., 2018). Evaluating the training and awareness program will allow the removal of inefficiencies and improve the training qualities. According to Yamin et al. (2020), performing after-action analysis on the security awareness and training program using the participants' feedback and event information helps maintain and manage the security exercise and environment.

Theme 2: The Use of Technical Control Mechanism

Overview

The second theme from the data analysis was the need to make use of technical control mechanisms. The responses from the participants and the organizational documents supported the use of technical control mechanisms. According to Molin et al. (2018), organizations deploy technical security measures (TSMs) to protect corporate assets from cyberattacks. Security controls are safeguards put in place to reduce the chances of threats exploiting a vulnerability. The lack of security control mechanisms puts the confidentiality, integrity, and availability of information at risk. TSMs include biometric devices, antivirus, digital signatures, firewalls, and other authentication protocols to protect the information system against cyberattacks (Gcaza et al., 2017). Table 4 below depicts references to the use of technical control mechanisms.

Table 4

References to the use of technical control mechanisms

Major themes	Participant		Document	
	Count	References	Count	References
Technical control mechanism	6	64	7	10

Findings From Participant Interviews

The second theme of the data analysis was the need to use technical control mechanisms to secure the SCADA systems. All the participants expressed a need to use technical control mechanisms as an objective in the organization's cybersecurity program. P1 mentioned the topology of the SCADA systems to include hardware level and software level and how to defend the system at both levels. According to P1,

> So the topology of the systems starts at the hardware level for security. It will come down to a firewall and strict firewall rules that are put in place to protect the SCADA system from outside intrusion. Secondly, network intrusion prevention systems have been used in the SCADA industry to ensure that unexpected network traffic can be halted and reported if something goes past the firewall. Finally, security comes down to the software level and managing your users. The majority of security attacks, to my knowledge, come from people accidentally or unintentionally giving out their passwords.

P3 also mentioned firewalls as part of standard security practice that organizations can use at a high level to limit the attack surface. P2 and P3 mentioned air gapping of sensitive systems. P2 stated that “isolating and air gapping, the SCADA system from the rest of the corporate environment, this is where IT operational technology environment, has grown and, and is taking off now.” The concept of air gapping ensures the physical isolation of a computer network from establishing an external connection. In the case of P3, “air gapping of sensitive systems, separate control of operations from corporate data access.” Another technical control mechanism mentioned by P1, P4, and P5 is encryption.

Data encryption converts data into another form that only people with the secret key or password can read. P5 mentioned that organizations depend on data encryption to secure data from the site, especially field devices. P5 stated that “Normally, they have more restricted access control in the corporate building, but the security level configuration is not well-executed in the rural area. They depend on the employees themselves and also on data encryption.” P4 mentioned encryption among the methods used to prevent security breaches on the SCADA systems’ networks. According to P4, “Use of encrypted transmission to clients. So between servers and clients, there are encrypted protocols or encryption protocol.” P1 said that some organizations use communication equipment that may or may not be encrypted.

> So from a field device, a lot of these customers use V-Sat or satellite communication, or even radio or cellular communications, that may or may not be encrypted. But I would think that that is not a very secure method. I would think if somebody wanted to take the data out of the air, whether that be from the V-SAT

> or cellular, that would be an easy method to be able to get into or see the data that is coming out of those field devices.

P1 mentioned using an intrusion detection system, while P2 mentioned the lack of and the consequences of not having one. P1 observed that “the network intrusion prevention systems have been used in the industry, the SCADA industry lately to ensure that if something does get past the firewall, unexpected network traffic can be halted and, and reported.” P2 gave an example of an organization that did not have IDSs.

> I can give you an example that I'm working on. I currently have a customer who is dealing with the after-effects of an intrusion. But this happened when they had nothing. They had no security policies, and they had no proper procedures and practices. They had no antivirus in the system. And as it turned out, the actual intrusion itself did not affect the SCADA system. It was some of the after-effects when they tried to implement some preventative measures. But that had negative side effects on the SCADA system.

P4 and P6 agreed on other technical control mechanisms such as two-factor authentication. Two-factor authentication requires two forms of identification to access information. The first factor is usually a password, and the second factor could be a code sent to a smartphone or biometrics using face, retina, or fingerprint. P5 and P4 also agreed on the use of Virtual Private Network (VPN). P4 stated that “We provide support remotely. So, VPN is a standard tool to establish a secure connection.” VPN services provide secure and encrypted connections, which ensure online privacy and anonymity. P1, P2, P5, and P6 mentioned antivirus or antimalware software. Antivirus software protects computer systems from malware and cybercriminals by scanning, detecting, and removing viruses. P6 stated that antivirus might be ineffective if not properly deployed. “for instance, deploying antivirus without understanding the impact that it will have on the system will degrade the system performance.” P2 mentioned whitelisting, a strategy that allows users to take actions on a computer system based on a limited set of functionality explicitly allowed by an administrator.

Organizational Documentation Support

Six organizational documents collected and analyzed supported the second theme of using technical control mechanisms to secure their information assets. In the first instance, the authors of O2D1 stated that they are aware of cybersecurity threats. They take these threats seriously by taking a layered security approach to mitigate the risk. The authors of O1D1 mentioned using appropriate and reasonable security measures to protect their information. The authors of O1D2 mentioned using intelligence monitoring and IDSs as part of security measures because disruption of their operation may impact the environment, public health, and the economy.

Document from partner organization 3 (O3D1) mentioned putting in place a robust enterprise risk management (ERM) program to identify technology and cybersecurity-related risks and ensure appropriate mitigating measures are in place. Authors of O3D3 maintained that they employed industry-standard security measures to protect their information assets. Authors of O2D3 stated that the security and protection of their information assets and databases are essential. Therefore, the organization monitors its infrastructure using stringent security protocols and a process that permits a quick response to adverse situations. According to the authors of O3D4, the organization has existing systems to monitor and mitigate cybersecurity risk. However, they continue developing, reviewing, and updating the system depending on the nature of the risk.

Framework Reference to the Conceptual and Other Scholarly Studies

I used GST as the conceptual lens from which I explored the strategies best suited to prevent security breaches in SCADA systems' networks. The evidence gathered from the study participants, organizational documentation, and existing literature supports the theme of using technical control mechanisms. A view of the theme of using technical control mechanisms through the lens of GST will holistically contribute to securing the SCADA systems’ networks. According to Malatji et al. (2020), organizations use numerous security frameworks to address the enterprise security challenge. These security frameworks help organizations to identify, protect, detect, respond, and recover from cyberattacks.

All six participants listed various technical controls such as two-factor authentication, VPN, antivirus, and whitelisting systems for protecting the SCADA systems. Bertalanffy (1972) stated that the different components of a system must function together as a whole to achieve its objectives. According to one participant, the SCADA can only be secure if all the technical control mechanisms work together and not in isolation. Organizations must utilize all the tools available to them to secure information assets. Due to the ever-changing technological landscape, organizations must stay up-to-date with the current trends, threats, and vulnerabilities. According to Jae-Myeong and Sugwon (2020), cyberattacks directed at the SCADA systems are becoming more intelligent and complex. Organizations must therefore take a proactive posture to secure their SCADA systems.

GST is a robust lens used to understand organizations' wholeness when all its components work together to achieve their goals (Simola, 2018). The strategies used by security managers to secure the SCADA systems in this study make up the organization. Security managers look at the organization as several subsystems working together to achieve a common objective. At the core of this objective is the protection of organizations’ information assets. Mar (2019) stated that a failure of a system’s part would prevent the entire system from functioning correctly. A failure by the security managers to deploy the appropriate technical control mechanism may result in the system's security failure. When security managers utilize the systems theory approach to securing their SCADA systems, they can apply a holistic approach and consider all the parts that constitute the SCADA systems while deploying technical controls.

Other scholarly studies are also in alignment with using technical control mechanisms to secure the SCADA systems. The use of technical control mechanisms involves deploying technology to monitor systems to reduce vulnerabilities (Fink et al., 2017). Technical control mechanisms are the first defense line against security threats in systems (Gopalakrishna-Remani et al., 2018). Technical control mechanisms include antivirus, encryption, firewalls, biometric devices, digital signatures, and other authentication protocols. Chen et al. (2019) stated that using data encryption is an indispensable step in protecting privacy. According to Fink et al. (2017), the process of safeguarding and protecting personal data and organizational information assets will improve with the use of technical control as a tool for systems hardening.`

It will benefit the SCADA system to have security mechanisms that can detect security threats in advance. Although technical control mechanisms alone may not be sufficient to prevent and deter data breaches from cyberattacks, they may serve as defense layers. According to Padilla and Freire (2019), organizations should include technical control mechanisms as part of their organizational policy to prevent economic damages that may result from cyberattacks. Selecting appropriate information security controls by security managers that permit the defense of information resources and assets is becoming difficult and complex. Tariq et al. (2020) asserted that selecting information security controls should be based on an appropriate level of security which requires intensive investigations regarding vulnerabilities, prevailing threats to the organization, budgetary considerations, and considerations for implementation and mitigation.

Organizations must continually evaluate the effectiveness of the security apparatus in place to ensure optimal results. According to Oakley (2019), some strategies devised to protect organizational information assets lose their vibrancy over time. By continuously evaluating the efficacy of these intervention methods, organizations can enhance the safety of their SCADA systems because they can determine the efficient techniques. Rong et al. (2019) mentioned that the main content of security evaluation includes identifying risks that information systems may face, the probability of the risks occurring, possible consequences, elimination strategies, and control strategies.

Security managers conduct vulnerability analysis or penetration testing of the connection to the SCADA network to evaluate the protection associated with these pathways. According to Kristiyanto and Ernastuti (2020), a penetration test assesses and evaluates network security by simulating attacks from the attacker's perspective. Security managers should use the information gathered from the penetration test and the risk analysis to develop a robust protection strategy for the SCADA networks. It is crucial to implement IDSs, firewall rules, and other security measures at every entry point since the SCADA network is only as secure as its weakest connecting point.

Reference to Effective Information Technology Practice

The following section of the study ties the theme of technical control mechanisms back to effective information technology practice. All the participants and some of the organizational documentation specified different security controls for securing the SCADA systems. According to Tidrea et al. (2019), SCADA systems are vulnerable to attacks on software, hardware, and communication protocols. Cyberattacks on the systems, if successful, can be catastrophic, impacting social safety and industry development. Maintaining the sanity and health of the SCADA system against cyberattacks poses intimidating challenges.

Security managers should evaluate the SCADA networks' security strength using vulnerability analysis or penetration tests and use these tests' results to develop a robust protection strategy for the system. Proposed security measures for the SCADA systems, according to Jae-Myeong and Sugwon (2020), are classified into three categories: (a) physical/logical network separation, (b) communication message security, and (c) security monitoring. The purpose of separating networks into different zones is to reduce the probability of successful attack thereby, mitigating attack impacts. The purpose of communication message security is to ensure confidentiality, integrity, the authenticity of messages exchanged in the system. At the same time, network monitoring involves detection and responding to network intrusions. Abou el Kalam (2021) recommended a holistic methodology that identifies security needs and objectives, specifies security models and policies, derives appropriate architecture, and implements reasonable security measures.

Security managers should be able to apply appropriate security measures to their systems. Technical control is a well-known network security mechanism for protecting a network (Mihalos et al., 2019). The participants mentioned the following technical controls: encryption, firewalls, two-factor authentication, VPN, antivirus, whitelisting systems, and IDSs. The technical control mechanism mentioned above and the holistic methodology earlier mentioned will help protect the SCADA systems against external and internal intrusions. Security managers should adopt a proactive approach that involves continuous improvement, testing, adaptation, and correction.

Attackers are using more sophisticated techniques to compromise the integrity of the SCADA systems. Security managers must use efficient and quick detection systems to observe events on the SCADA networks for signs of unusual incidents (Yadav & Paul, 2021). The intrusion detection strategy should alert security managers of malicious network activities from internal or external sources. Security managers should also put in place incident response procedures to allow an effective response to an attack (Abou el

Kalam, 2021). Enabling logging on all systems and daily auditing the system logs will complement network monitoring and suspicious activity detection.

Another approach security managers may use to prevent security breaches on the SCADA systems networks is to deploy firewall rules to prohibit access. Zheng et al. (2020) recommended a firewall configuration as one of the defense strategies to prevent DoS attacks. The firewall rule must be as specific as possible when permitting approved connections. For example, an operator should not have blanket network access just because of the need to connect to a particular component of the SCADA systems. According to Patel (2020), a single firewall may not be reliable and efficient in providing the needed protection for organizational networks. The combination of firewalls with the implementation of other security measures will provide security layers and make it difficult for cyber attackers to access the SCADA networks.

Implementing patch management is another strategy security managers can use to prevent and lessen data breaches. According to Jacobs et al. (2020), IT professionals deploy patches to update, fix, and improve vulnerabilities within an organization’s networks. Security updates primarily fix bugs and enhance network security. Some bugs in the network present security risks, and updates can quickly address these security risks. Furthermore, security updates can fix vulnerabilities to new attacks not detected during the software's initial release. According to Avery and Wallrabenstein (2018), implementing patch management assists security managers in organizations to fix bugs found within their networks. Security breaches are preventable if systems are up to date with appropriate patches (Hayhurst, 2018). Security managers should apply new patches as soon as possible once vendors release their monthly updates since these patches resolve the latest known exploits and vulnerabilities.

By leveraging and using technical control mechanisms, organizations can harden and improve the function of protecting and safeguarding their information assets and condensing surface vulnerabilities. Because of the vast amount of information transmitted on the SCADA systems' networks, security managers must know how to keep this information safe.

Theme 3: Standard Security Policies

Overview

The third theme that emerged during the data analysis stage of the study was standard security policies. The protection of an organization's information assets is an integral part of its business. With standard security policies and best practices, security managers can protect SCADA networks and end-users from malicious attacks. According to Rostami et al. (2020), information security policy is crucial when implementing information security. Information has increasing value in today's organizational environment, and new methods of maliciously using this information are evolving. As a result, organizations are looking for ways to protect their data from cyberattacks. Security standards such as ISO27001 mandated information security policies for information security management. (Paananen et al., 2020). Information from Table 5 below shows the number of references related to standard security policies.

Table 5

References to Standard Security Policies

Major themes	Participant		Document	
	Count	References	Count	References
Standard Security Policies	5	48	7	10

Findings from Participant Interviews

Five of the participants mentioned having standard security policies. Leaders must formulate and establish security policies that outline how users can interact safely with data by ensuring procedures and policies are in place to stop hackers (Alhassan et al., 2019). According to participant P1, an organization must ensure that proper group policies are in place. P1 stated that:

> Security comes down to the software level and managing your users most of the security attacks, to my knowledge, comes from people accidentally or unintentionally giving out their passwords. So, ensuring that's locked down and ensuring proper group policies are in place. So, users have to change their passwords frequently is good practice for inside the environment.

Participant P4 mentioned having a policy that ensures regular password change, such as a password rotation policy. That way, someone who used to work at the company three months ago doesn't still remember passwords that haven't changed. P1 further stated that there should be a strict policy regarding removing Active Directory and corporate access once an employee leaves.

Participant P3 stated that technical controls are inadequate without well-defined policies, well-defined procedures, and well-described requirements. P3 noted that "policies and practices and procedures drive the technical and also drive awareness." Participant P5 also agreed that formal strategies equal company policy and regulations, which will also impact technologies. Participant P2 stated that "standard security practices such as hardware and software, firewalls, air gapping of sensitive systems, separating control of operations from corporate data access, those are all high-level strategies that a customer uses to limit the attack surface on these systems." Participant P2 stated that organizations should back up the policies with a technical execution plan. P2, when further to give an example that employees should not be sharing passwords. P4 also spoke about having an excellent password policy:

> You can have a great password policy, and then have somebody who's not respecting it write it on sticky notes and pasting them to their monitor for everybody to see. Or somebody who will send you the latest password update by unencrypted, you know, messenger chat or something like that.

A good password policy enhances computer security by allowing users to use strong passwords. The passwords must not contain personal information such as the user's real name, company name, and username. A strong password should contain different characters, including uppercase letters, numbers, lower case letters, and special characters.

P3 stated that organizations should make use of a feedback loop while defining policies and procedures. P3 went further to explain the feedback loop in the following statement:

> The feedback loop is when you take, and you start to define what your actual policies and procedures are, and you're talking to people, they'll come back and say, Well, that's all well and fine. But I need to be able to do this role as part of my job. So that then needs to be incorporated back into your policies and procedures. So, you don't dictate what the policies and procedures are. You develop them in conjunction with the people who are affected.

P3 stated that part of the things organizations have to put into place as part of the policies is to ensure someone is responsible for managing, maintaining, monitoring, and controlling processes. The following statements detailed the example given by P3 regarding defining responsibilities.

> So, if I wanted to make a change to a system, for example, I have to go to you and say, here's what I want to do, here's how I'm going to do it, and so forth. But I need to get that approved first. So that I'm not just running off and willy nilly making changes. So, the enforcement is part of the policies and procedures because you have to define responsibilities in there as to whose duty it is to perform or approve.

Most times, employees do not comply with organizational policies and procedures. P4 stated that employees should not be intimidated to call each other out when they observe sloppy practices.

Organizational Documentation Support

The reviewed documents support the use of standard security policies to prevent cyberattacks and other risks to digital networks. According to the authors of O2D7, employees using company communication vehicles must follow their cybersecurity policies to prevent viruses, hacking, and other security threats. The authors of O1D3 stated that their policy complied with all applicable laws and is updated periodically. Both the authors of O3D1 and O2D6 agreed with this assertion. According to the authors of O3D1, the organization routinely evaluates its policies and procedures annually, but mostly as needed, proving to be very effective. In the same vein, the authors of O2D6 stated that they continue to update policies and standards to keep up with new threats.

The company information systems specified by the authors of O1D1 include computers, phones, mobile devices, internet access, storage devices, email, software, and applications. The use of these devices should be consistent with the company policies. To prevent security threats, employees should make use of organizational assets only for company business. According to the authors of O3D4, a significant cybersecurity incident could negatively affect their operations; therefore, they routinely perform systems updates. The authors of O3D3 stated that they retain information as long as required and relevant to their operations but employ industry-standard security measures to protect the information. The authors of O3D3 noted that they use data retention and deletion policies to dispose of information when no longer required.

Reference to the Conceptual Framework and Other Scholarly Studies

The theme standard security policies align with GST, which was the conceptual framework for this study. An organization that deployed standard security policies will contribute to the success of the organization. According to Abraham and Nair (2018), information security is an organization's critical business part. A breakdown in the security defense occurs when security components do not function as a system. I used GST in this study to show how the information security strategies presented will help organizations accomplish their objectives. According to Hartnell et al. (2019), an organization system consists of various highly interdependent components. The collaboration of these interdependent components must function appropriately to bring about the accomplishment of organizational goals. Some of the participants mentioned that technical controls are inadequate without well-defined policies and procedures. Information security policies must align with the business to bridge lapses in information security that could lead to a security breach.

Any information security system that fails to function in its entirety will break its defenses. According to Bertalanffy (1972), the system's various components must work together to accomplish the primary goal. Standard security policy is one of the security apparatus required by an organization to mitigate data breaches. Five of the participants indicated that employing standard security policies could safeguard and reduce data breaches. Since standard security policies are an integral part of the security system, assessment and modification with a holistic approach will prevent system failure. This study's findings indicate that by utilizing the GST approach to information security with standard security policies, security managers can ensure the organization’s information assets are safe from cyberattacks.

This study’s findings demonstrate how standard security policies align with existing scholarly studies. According to Palanisamy et al. (2020), many security breaches arise from non-compliance with security policy. These documents are the foundation of information security, which addresses the security footprint of the organization. As observed by two of the study participants, technical controls are inadequate without well-defined security policies. According to a recent article, information security threats may be reduced if organizations design and implement information security policies to regulate employee security behavior (Trang, & Nastjuk, 2021).

In one of the participants' examples concerning the after-effects of an intrusion regarding an organization, P2 stated that the intrusion occurred because the organization had no proper procedures and practices. The SCADA systems' interconnectivity to the internet and other devices exposes their vulnerabilities, increasing their security risks. According to Rostami et al. (2020), information security policy is one of the keys to adequate information security. A security policy is not valuable for an organization that refused to implement the guidelines and regulations within the policies. According to Trang and Nastjuk (2021), an employee’s behavior may constitute a significant threat to an organization's security system because they have access to knowledge of the organizational process that may enable cyber attackers to exploit weaknesses. An employee’s security behavior may pose a significant risk to organizational security if they deviate from the prescribed behavior in the policy. Paananen et al. (2020) stated that employees might find it challenging to follow policies due to inconsistent explanation of the controls, inadequate explanation and use of terms, and unexplained policy architecture.

The harm to the information system from an employee may be due to negligence or non-compliance with security policies (Sharma & Warkentin, 2019). All employees from the chief executive office down to the newest employee must comply with the policies. Mistrust toward compliance with security policy may occur if upper management does not comply and the organization does not enforce the consequences of non-compliance. According to Wang and Xu (2021), employees will likely comply with information security policies when they perceive that the chance of being punished is higher and deterrence is more severe. Security managers must ensure that all employees read and acknowledge the security policies. The policy should include a statement stating that noncompliance with the policies may lead to sanctions and administrative actions, including employment termination. Acknowledgment of this statement by the employees will strengthen the enforceability of the policy. The extant literature that I reviewed for this study aligns with the findings and highlights the importance of standard security policies.

Reference to Effective Information Technology Practice

Five of the participants mentioned the importance of using standard information security policies. While some of the reviewed organizational documents also attested to this fact. Recent literature reviewed buttress the theme of standard security policies as a strategy SCADA security managers can deploy to prevent data breaches on the SCADA systems’ networks. Information security policy addresses security issues within an organization by defining individuals' responsibilities and roles to protect the organization’s information assets (Wiafe et al., 2020). Security policies describe acceptable use of organizational information resources as well as consequences when violated. The main idea is security enhancement within the organization when employees comply with security policies.

One of the significant purposes of a security policy is to protect organizations and their employees. According to Chapman (2021), having a security policy in place will lay down guidelines and standard protocols for all employees to follow, whether remote or office-based. A clear understanding of the role a security policy plays in the organization will enable employees to act accordingly and be held accountable for their actions. Employees should not fear reprisal, and they are protected as long as they comply with the defined security policies. According to Bansal et al. (2020), the policies should include formal guidelines, procedures for monitoring, and methods for ensuring compliance, such as punishment for non-compliance and rewards for compliance.

Organizations must ensure that employees comply and actively follow security policies, and the security policies must also be up to date (Bauer et al., 2017). Security managers should employ an administrative approach to enforce IT security compliance by employees. Organizations may use punitive measures to dissuade users from not complying with security policies and standards. According to Trang and Nastjuk (2021), one of the standard measures to encourage employees to comply with security policies is punishments and rewards. Organizations can control the behavior of their employees with the threat of punishment and rewards. Employees must comply with security policy since the security policy's objective is to provide management direction and ensure information security. Security policy is only effective when employees comply and adhere to it.

A good security policy must be usable and comprise of many factors. According to Ali et al. (2020), the design of the security policies should be according to every level of the organization. Input should be from all top-level down to the bottom level of the organization. The involvement of all stakeholders in the development of the document is essential. A weak security policy design may cause employees to perform actions that are detrimental to their organization and lack protection for subtle data (Alqahtani, 2017). The inclusion of all stakeholders in the development process of the security policy will encourage employees to define the work conditions and rules under which they must work (Niemimaa & Niemimaa, 2019).

Another aspect is to ensure that security policies are up to date and regularly updated. The dynamic nature of security risks necessitates the development of proactive approaches to information security. Also, continuous performance and changes in an organization require evaluation of security policies and procedures to ensure that they work according to predefined criteria and indicators (AlGhamdi et al., 2020). A crucial part of organizational success is to review their security policies regularly. Although the security policies' core elements may remain the same, the policy's details must grow and adapt with the industry and the organization. The policies need to change because old policies may fail to comply with new regulations and laws. SCADA security managers should review security policies to ensure compliance with technology, regulations, and security best practices.

Theme 4: Access and Identity Management

Overview

The fourth major theme that emerged during the analysis phase of the study is access and identity management. Ascertaining users' identities is crucial to security managers to determine who is accessing the SCADA systems and organizational information assets. The findings demonstrated that access and identity management is essential to authenticate users over SCADA networks securely. According to Chia and Chin (2020), an identification scheme allows an entity to assert its own identity to another entity through corroborative pieces of evidence. Security managers use an authentication mechanism to request login credentials such as usernames and passwords from employees, contractors, or vendors before accessing the organization’s information assets. The primary aim is to protect information assets from security threats by enforcing authentication measures. Users' identities may be verified using various authentication forms such as two-factor authentication, multi-factor authentication, or usernames and passwords. Table 6 below depicts the number of references related to the use of access and identity management.

Table 6

References to the use of access and identity management

Major themes	Participant		Document	
	Count	References	Count	References

Access and Identity Management	6	44	6	8

Findings from Participant Interviews

The fourth theme of the data analysis was access and identity management to secure the SCADA systems' networks. All the participants expressed the need to use an access control mechanism to safeguard the system from internal and external cyberattacks. According to participant P1, most security attacks come from people accidentally or unintentionally giving out their passwords. P1 recommended that proper policies concerning frequent password change is good practice within the SCADA environment. P2 and P4 also supported the notion of frequent and regular password changes. P2 mentioned that users should not be sharing passwords, especially employees giving out their passwords and asking other people to act on their behalf, a notion that P1 also supported.

Users must understand the importance and the severity of securing the SCADA system. According to P4, "it's important that employees who are accessing these systems and representing the company and working with, you know, critical infrastructure that they understand the severity of the security and they need to take it seriously." P1 stated that there should be a strict policy regarding removing Active Directory and corporate access immediately after an employee leaves an organization. P3 also supported the deactivation of the account of employees immediately after they stopped working for the organization. P4 also stated that the organizations should ensure ex-employees do not have an active account. P4 mentioned notifying customers of an employee's exit from the organization so that customer organization can remove their accounts from the user's list.

Another point that four of the participants agreed to is the use of Active Directory to control access. According to P2, an organization should make use of the least privileged philosophy approach for user security. P2 stated, "In other words, users only have access to the things necessary to complete their tasks, and nothing more." This principle, according to P2, is a high-level strategy that an organization uses to limit the attack surface of the SCADA systems. P3 stated that organizations could use Active Directory to tailor the roles assigned to people down to their requirements only. Active Directory use will prevent users from seeing or operating on data they do not have the authority to access. P5 also mentioned controlling each user's privileges using the Active Directory. P6 stated that "From an Active Directory standpoint, permissions should be controlled and limited to exactly what the role of the employees and nothing more."

P4, P5, and P6 supported other authentication methods such as VPN to authenticate, two-factor authentication, a badge to enter a building physically, and a shared screen session to avoid physical contact with the SCADA systems. P2 stated that:

> More recently, they've been making wide use of two-factor authentication. It is not just a username, password but also a temporary pin that appears on a token generator on my cell phone. Some customers have a hard disconnect like they turn off their VPN when it's not in use or disable user accounts when they're not in use.

P6 mentioned using a security badge to access an office building physically. Lastly, P6 said the use of a shared screen limits contact with the SCADA systems physically.

Organizational Documentation Support

Five of the corporate documents analyzed are in support of the use of access and identity management. According to the authors of O1D2, the impact on public health, the economy, and the environment will be significant due to pipeline operations' disruption caused by security threats. Hence, the organization uses an access control system to dictate who can use and access company information and resources. The authors of corporate document O1D3 stated the organization's commitment to securing customer information through administrative, technical, and physical safeguards to protect its information assets from unauthorized access, destruction, alteration, use, or disclosure.

Authors of O2D5 stated that the organization employed complex passwords as one of the many ways to protect information and physical assets. The authors of O1D3 reiterated that they would never demand a user password or ask users to send their passwords to another person or company through e-mail. Authors of document O3D3 emphasized the need for users of services to secure their passwords, user-id, or other authentication forms used for accessing secure areas of digital services. The authors of O3D3 also stated that access to a protected area of any of their services is only for authorized users. The authors of O2D6 mentioned using technology to increase speed and access to information assets.

Reference to the Conceptual Framework and Other Scholarly Studies

GST, which served as the conceptual framework, is also relevant to the last theme, access and identity management. The framework supports the fourth theme's findings since the conceptual framework addressed the importance of developing security measures regarding preventing unauthorized access to information assets. Holism, a fundamental concept of GST, emphasized assessing the system's components as a whole and not through its components (Van Assche et al., 2019). Evidence from the study's findings identified access and identity management as part of the whole security system. Indu et al. (2018) asserted that vulnerabilities in identity management systems cause many information security issues. Participant P1 also agreed with the notion that most security attacks emanate from users who accidentally or unintentionally gave out their password information. The assertion made by Indu et al. links the findings of my study back to the GST as the conceptual framework for this study.

The process of accessing a system within a specific structure following an implemented process that permits or rejects access or monitors users' activity strengthens the target system's security. According to Sindiren and Ciylan (2019), adjusting authorizations assigned to users ensures they only have access at the authorized level, ensuring data privacy and integrity. According to P2, SCADA administrators have the highest access levels, which may not be the best security posture. The least privilege principle would have been appropriate, which would allow access based on the user's role and job duties. The deployment of various access and identity management mechanisms such as two-factor authentication, multi-factor authentication, or usernames and passwords may ensure authentication, accountability, and authorization. GST, therefore, explains how the SCADA systems could be more secure from malicious attacks using various access and identity management mechanisms.

Other scholarly articles support the theme of the use of access and identity management. The lack of authentication and limiting users' access to the SCADA systems’ networks may result in the loss of confidentiality, integrity, and data availability. According to Lal et al. (2017), user access management is a control strategy to help maintain networks and deter negligent and malicious threats. Users could be employees, customers, vendors, and partners. According to Schrimpf et al. (2021), organizations of various types are becoming exposed to information technology-related threats, and IAM is adequate information security to defend against them. Participant P4 stated that employees accessing the SCADA systems should understand the severity of the system's security and take it seriously. The overarching purpose of access and identity management is to grant access to organization information assets that users have rights to in each context, including onboarding users, permission authorizations, and offboarding users promptly.

The strength of the password is essential in the defense against unauthorized access to organizational information assets. Current scholarly articles reiterated that a password must include a combination of numbers, letters, and special characters. The weaker the password's strength, the less protected the system will be from hackers and malicious software (Guo & Zhang, 2018). Passwords are the first line of defense against unauthorized access to the SCADA systems. Security managers should maintain stronger passwords for all accounts on the system. According to Guo et al. (2019), users often create predictable passwords to meet password composition policies, making passwords easy to remember, thereby reducing the passwords' strength. Some users also write down complex passwords, which may cause the passwords to be compromised. Xu and Han (2019) stated that the combination of letters, numbers, and special characters are ways to prevent weak authentication. Security managers should enforce a strong password and make sure that the employees comply with this policy.

Proper management of user access will help maintain SCADA systems' networks and deter negligent and malicious threats. The deployment of access and identity management mechanisms, according to Pol (2019), is crucial to detecting and preventing data breaches that may result from unauthorized access. P3, P5, and P6 all asserted that using Active Directory to control access to organization information assets will prevent users from seeing or operating on data they do not have the authority to access. The scholarly articles reviewed aligned with the study's finding that access and identity management mechanisms are data security strategies organizations can use to prevent security breaches caused by malicious attackers on the SCADA systems' networks.

Reference to Effective Information Technology Practice

This study ties the fourth theme, access, and identity management, to effective information practice. According to Blythe and Coventry (2018), organizations need to implement security management tools to ensure their network and systems' security and prevent unauthorized access from internal and external sources. Access and identity management mechanism is a security management tool that organizations may use to control unauthorized SCADA systems access. The first security defense layer is access and identity management that privileged and nonprivileged users pass through to access a system. All six participants and the reviewed documents indicated support for using a form of access and identity management mechanism to control and minimize malicious threats, leading to data breaches.

One of the strategies used to address security challenges on a systems' network is passwords. According to Xiaobo et al. (2019), some strategies to address security challenges on a computer network include a hard-to-crack password and user credentials to prevent unauthorized network access. Security managers should limit access to sensitive information only to those who need the information to fulfill their organization's duties. P6 supported the use of Active Directory to control and restrict user's permissions to their exact role within the organization. Organizations should tailor access and authority granted to users specific to their assigned roles.

The type of authentication method deployed is crucial to protecting the SCADA systems' networks. The deployment of username and password coupled with two-factor authentication can prevent unauthorized access. Wang et al. (2018) prescribed a two-factor authentication method to control access to a network. One of the participants also supported the use of two-factor authentication. Two-factor authentication provides an extra layer of security that ensures that the person trying to access it is legitimate. The spread of Covid-19 has forced many organizations to introduce preventive measures such as allowing their workforce to work from home. Technology has enabled businesses that would have grounded to a halt to continue. According to Sarginson (2020), multi-factor authentication played an essential role in offering authentication protocols that work for employees while providing the right level of protection for systems, networks, and data.

Security managers should deploy tools to monitor accounts and authorize access rights. Part of the access and identity management involves periodic review and evaluation of access rights for all employees and vendors within the organization. A user access review includes assessing user roles, access rights and privileges, and user credentials. Thomas and Galligher (2018) observed that the access rights of users should be added, modified, or removed when users change position or exit the organization. Users may hold access rights that are no longer necessary without proper monitoring, leading to unauthorized access to data (Thomas & Galligher, 2018). According to Gaurav et al. (2020), user access control consists of two components: authentication and authorization. The authentication process involves allowing access only to the intended user, while the authorization process involves allowing users access to data as decided by authorization policy.

Passwords for authenticating users are susceptible to attacks such as shoulder-surfing attacks, where attackers can learn the user's password. Some of the participants recommended regular password change as good practice within the SCADA environment. According to Yu et al. (2017), a periodical password change will render the previous password useless. One of the participants also advocated for using a complex password as one of the many ways to protect information and assets. Wang et al. (2019) stated that identity management could be problematic in a system when defects persist in the design since it could lead to a data breach. Since access and identity management is the first technical defense layer users go through to access a system, security managers should ensure they follow best security practices during deployment to minimize direct risks of a data breach that may occur.

Applications to Professional Practice

The challenges to protecting the SCADA systems from data breaches have increased over the years. SCADA security managers find it increasingly difficult to find the best security approach to protecting these systems due to their vulnerabilities and cybercriminals' activities. The system is at high risk of being attacked by cybercriminals due to the interconnected devices which exposed its vulnerabilities. Consequently, security managers must develop security schemes to address SCADA systems' vulnerabilities and implement security strategies to combat various threats. This study's findings are significant to Information Security practitioners, IT compliance, and training professionals in cybersecurity. IT and compliance professionals and SCADA security managers will benefit from these findings if they use the strategies revealed in this study to mitigate security threats to SCADA systems. The study revealed important information that prepares security managers with the essential knowledge necessary to improve cybersecurity strategy and include new IT compliance and cybersecurity training ideas. The improved security practices will help mitigate threats to the system and strengthen cybersecurity protection to prevent cyberattacks.

A new breed of cyberattacks resulted from the continuous integration of the SCADA systems to sophisticated technologies (Genge et al., 2019). This new breed of cyberattacks applies sophisticated knowledge and understanding of the SCADA systems to lunch a successful attack. This study's findings may help security managers plan and implement strategies to meet this new breed of cyberattacks against the SCADA systems. The study revealed four themes, which are (a) the importance of security awareness and workforce security training, (b) the use of technical control mechanisms, (c) the establishment of standard security policies, and (d) the use of access and identity management techniques. These present four themes are keys to a successful strategy to protect the SCADA systems and ensure compliance with organizational security policies.

The presented themes are essential to securing SCADA systems. Security managers may use this knowledge to improve their cybersecurity strategies in SCADA systems environments and conventional IT practices. A breached SCADA system can lead to disruption of the physical process, resulting in severe economic consequences. Security managers may use this study's findings to improve their knowledge and understanding of securing the SCADA systems. An effective cybersecurity management strategy can improve the security culture and posture of an organization. Therefore, this study's key themes may improve the current tools and techniques to mitigate cyber threats and successful SCADA systems' breaches.

Implications for Social Change

This study's findings contribute to the existing body of knowledge and literature on security management strategies for securing the SCADA systems’ networks, thereby preventing security breaches. This study's findings may also have positive social implications by increasing the trust and confidence the society and community have in the services provided by SCADA systems due to improved protection of the system. Cyberattacks on the SCADA/ICS systems constitute severe threats to critical industrial facilities like the power grid due to their catastrophic impact on industry development and social safety. Therefore, security managers should ensure that the SCADA data is untampered with, always available, and accessible to authorized users only. It is necessary to develop and implement continuously reviewed and updated processes and procedures to ensure the SCADA system meets the criteria specified above.

The study's findings revealed essential factors that may help prepare security managers with the knowledge and strategies required to enhance the security of the SCADA systems' networks. The lack of understanding of vulnerabilities in a system will prevent security managers from providing effective network security defense to prevent cyberattacks on their networks (Loukaka & Rahman, 2017). The security managers' ability to defend the system against cyberattacks would depend on their skill sets, tools, knowledge, and stakeholders' buy-in. According to Butavicius et al. (2020), total dependence on technological security solutions alone will not adequately protect the systems. We cannot undermine the human factor associated with good security behavior to better predict vulnerabilities and design training and education programs to address these factors.

The findings of this study encompass technological security solutions and human factors associated with good security behaviors. The technical control mechanisms mentioned include antivirus, firewalls, two-factor authentication, access, and identity management. In contrast, the human factor consists of security awareness and security training, and the deployment of standard security policies. Although technical controls may prevent cyberattacks on the SCADA systems' networks, no technology can provide absolute protection when employees or users act less securely.

This study's findings will contribute to society by ensuring the confidentiality, integrity, and availability of the SCADA systems. It will also help avert the disastrous consequences for national security, national economy, and public health safety resulting from the system's downtime. The findings will also benefit security managers by increasing their knowledge and understanding of cyberattacks and cybersecurity, leading to secure SCADA systems. Also, the key themes identified and discussed will empower the pursuit of improved security practices. Finally, this study's strategies will improve security practices to facilitate using current techniques, methodologies, and tools to mitigate cyberattacks against the SCADA systems.

Recommendations for Action

SCADA security managers might benefit from this study's findings since the study presented some strategies that they could implement to prevent security breaches on SCADA systems' networks. SCADA security managers are at the forefront of mitigating cybersecurity threats because the critical elements of the SCADA systems, such as the PLCs, RTU, and other field elements, are remotely accessed using a WAN connection. Thus, SCADA security managers may benefit from this study since the strategies identified in this study can enable them or contribute during strategic planning and implementation. The strategies uncovered in this study contribute to the existing body of knowledge for securing the SCADA systems.

The first recommendation involves creating the importance of security awareness and workforce security training. The majority of cyberattacks aimed to exploit the human factor through social engineering, spear-phishing, malware, and ransomware. Since people are easier to compromise and influence, the study participants emphasized robust cyber-security training to protect employees and the organization from cyber threats and attacks. The study participants noted that training empowers employees with the knowledge on how to identify and mitigate cyber threats. According to the study participants, the training should be relevant, practical, flexible, and hands-on to strengthen the security chain's most vulnerable link.

The second recommendation calls for SCADA security managers to use technical control mechanisms for securing their SCADA systems’ networks. Some of the technical controls recommended by the participants include firewall and strict firewall rules. The firewall will monitor traffic, protect against trojans, hackers, and provide better privacy for the system. Another technical control mechanism is the IDSs to control access to the SCADA systems’ networks and prevent abuse and attack. The participants also mentioned air gapping to isolate the system from the rest of the corporate environment. Others are data encryption to safeguard transmitted data, VPN to ensure secure and encrypted connections, and two-factor authentication to provide authentication, accountability, and authorization. Organizations should provide security managers with the necessary tools to secure the SCADA systems and the essential training and knowledge required to discharge their duties. Security managers must stay up to date with the current trends due to the constantly changing technological landscape.

The third recommendation calls for security managers to implement standard security policies and circulate among the employees. Security managers should update the security policies regularly to keep up with emerging cyber threats. The security policies should include guidance broken into achievable tasks. I also recommend that the security policies have procedures to investigate breaches of policy, enforcement, and testing controls. Security managers should administer disciplinary action for intentional infringement or carelessness of cybersecurity policy. They should treat an accidental breach as an opportunity to conduct cybersecurity awareness training, while intentional breach or negligence should receive disciplinary actions. Disciplinary actions for noncompliance with cybersecurity policies should be equitable. SCADA security managers should not allow the employee's stature, either senior or middle management, to insulate them from other employees' consequences.

Finally, the fourth recommendation calls for an access and identity management mechanism to safeguard the system from internal and external attacks. I recommend the reevaluation of single sign-on and two-factor authentication. Hackers may bypass weaker identification measures through keylogging techniques, intercepting codes, and exploiting account recovery systems. A multifaceted approach for access and identity management, which includes multiple criteria for identifying users.

I plan to approach the dissemination of the study through multiple techniques. First, I will disseminate the summary of my research to all participants after the CAO approval. I will also present the findings through scholarly and technical publications such as the ProQuest database. My immediate goal is to publish and make my final study available for public searches, especially when organizations using the SCADA systems search for strategies to prevent data breaches on the SCADA systems' networks. I intend to share my research study where possible as a long-term goal using appropriate platforms such as my workplace, professional conferences, seminars, critical infrastructure workforce development, and training.

Recommendations for Further Research

I mentioned various limitations in earlier sections of this study. One limitation is that security managers may limit the information they shared due to SCADA systems' privacy and security. Further studies may expand to SCADA systems' software developers, especially integrating security into the solution. A study around this topic may help determine how cybercriminals use worms and viruses to exploit human interfaces, operations, and software design vulnerabilities. Furthermore, this study's conceptual framework was the GST, first proposed by the scholar Bertalanffy (1972) in 1946. Further studies could use other conceptual frameworks such as routine activity theory (RAT), developed by Cohen and Felson (1979) in 1979. RAT is premised on the following three principles that must exist together for a threat to result in an incident: (a) existence of an offender, (b) prevention or lack of prevention, and (c) a location (Cohen & Felson, 1979).

This study focused on oil and gas organizations in the midstream sector in the Southwest region of the United States. Further studies may be expanded to other organizations that use the SCADA systems to support their critical infrastructures such as water and electricity and other United States regions. Further research in this area will determine if these other organizations apply similar or different approaches to this specific IT problem. Although this study has contributed to the literature, a different research design or method may also be beneficial. The relationship between the SCADA security managers' strategies to secure the systems’ networks and the organization's support to ensure security may be examined using quantitative study.

Reflections

As I embarked on the DIT doctoral program, my goal was to understand better how to prevent security breaches in SCADA systems’ networks. The DIT program, although rigorous and demanding, has been a rewarding challenge. I learned how to conduct scholarly academic research and understand its implications and positive contributions to society. The two DIT residencies hosted by Walden University helped establish my research foundation, research focus, and understanding of various research methodologies and designs. The data collection process exposed me to interact with professionals who are passionate about securing the SCADA systems. Simultaneously, both the data collection and the research study's analysis phase exposed me to the rigors associated with the research process.

I was almost discouraged when I could not move past section 2 of this study after several review iterations. I discovered that the comments and the evaluations were helpful since the University research reviewer had little to correct. I had the opportunity to relate with professionals working with the SCADA systems, who are passionate about securing the systems during the data collection and analysis phase. The professionals inspired and motivated me with their positive attitudes and their enthusiasm to share their ideas and experiences in this study. All preconceived notions or potential biases that I may have had were mitigated by leveraging interview protocol during the data collection process. I also used member checking to verify my data interpretations to eliminate any bias I must have introduced while interpreting the data.

At the beginning of the research process, I thought I had enough insight into security incidents that may cause data breaches in the SCADA systems. During the research process, I uncovered new ideas and different viewpoints from the participants, which further broadens my knowledge. I have also gained an understanding and awareness of the research process and improved my academic writing skills. The research process also helped me develop specific competencies such as having clear objectives, proper planning, patience, teamwork, and a positive attitude. Finally, I have to mention my Doctoral Study Chair's guidance, which helped me navigate this study to a conclusive end. I cannot help but mention the school resources such as the library, writing center, and the center for research quality which provided the necessary writing assistance needed to succeed with the Doctoral Study.

Summary and Study Conclusions

The purpose of my qualitative multiple case study was to explore the strategies security managers used to prevent security breaches in SCADA systems’ networks. The SCADA systems’ networks are like other networks threatened by cyber-attacks that could quickly disrupt the nation’s critical infrastructure with severe consequences if the proper security is not in place. A cyber-physical attack of the SCADA system can disrupt the physical process, resulting in severe economic effects, equipment damage, safety, or security ramifications. Every organization that makes use of the SCADA systems is vulnerable to SCADA security threats. The following are specific threats to SCADA networks: (a) hackers, (b) malware, (c) terrorists, and (d) employees. The study revealed the following four principal themes related to security strategies used in preventing security breaches in SCADA Systems’ Networks from interviewing these participants: (a) the importance of security awareness and workforce security training, (b) the use of technical control mechanism, (c) establishment of standard security policies, and (d) the use of access and identity management techniques.

The data used in this study came from oil and gas midstream companies located in the Southwest region of the United States. I leveraged methodological triangulation to combine interviews, organizational documents, member checking, and observations to answer the research question. The participants have successfully prevented data breaches from the security management strategies implemented in their respective organizations in this study. This study's identified themes may impact other organizations' security management strategies to prevent security breaches in SCADA systems. This study's findings and conclusion may contribute positively to social change since the strategy may be implemented by other organizations using the SCADA systems to prevent security breaches on their SCADA systems’ networks.

References

Abou el Kalam, A. (2021). Securing SCADA and critical industrial systems: From needs to security mechanisms. *International Journal of Critical Infrastructure Protection*, *32*. https://doi.org/10.1016/j.ijcip.2020.100394

Abraham, S., & Chengalur-Smith, I. (2019). Evaluating the effectiveness of learner-controlled information security training. *Computers & Security*, *87*. https://doi.org/10.1016/j.cose.2019.101586

Abraham, S., & Nair, S. (2018). Comparative analysis and patch optimization using the cyber security analytics framework. *Journal of Defense Modeling & Simulation*, *15*(2), 161. https://doi.org/10.1177/1548512917705743

Adaba, G. B., & Kebebew, Y. (2018). Improving a health information system for real-time data entries: An action research project using socio-technical systems theory. *Informatics for Health & Social Care*, *43*(2), 159–171. https://doi.org/10.1080/17538157.2017.1290638

Ahanger, T. A., & Aljumah, A. (2019). Internet of Things: A comprehensive study of security issues and defense mechanisms. *IEEE Access,* 11020-11028. https://doi.org/10.1109/ACCESS.2018.2876939

Ahmad, A., Webb, J., Desouza, K. C., & Boorman, J. (2019). Strategically-motivated advanced persistent threat: Definition, process, tactics and a disinformation model of counterattack. *Computers & Security*, *86*, 402–418. https://doi.org/10.1016/j.cose.2019.07.001

Alfakhri, D., Harness, D., Nicholson, J., & Harness, T. (2018). The role of aesthetics and design in hotelscape: A phenomenological investigation of cosmopolitan consumers. *Journal of Business Research*, *85*, 523–531. https://doi.org/10.1016/j.jbusres.2017.10.031

Alfandari, R. (2019). Approaching the study of cyberbullying towards social workers from a systems perspective. *Aggression and Violent Behavior*, *48*, 60–64. https://doi.org/10.1016/j.avb.2019.08.004

AlGhamdi, S., Win, K. T., & Vlahu-Gjorgievska, E. (2020). Information security governance challenges and critical success factors: Systematic review. *Computers & Security*, *99*. https://doi.org/10.1016/j.cose.2020.102030

Alhassan, I., Sammon, D., & Daly, M. (2019). Critical success factors for data governance: A theory-building approach. *Information Systems Management*, *36*(2), 98-110. https://doi.org/10.1080/10580530.2019.1589670

Ali, R. F., Dominic, P. D. D., & Ali, K. (2020). Organizational governance, social bonds and information security policy compliance: A perspective towards oil and gas employees. *Sustainability (2071-1050)*, *12*(20), 8576

Allred, P. D., Maxwell, G. M., & Skrla, L. (2017). What women know: Perceptions of seven female superintendents. *Advancing Women in Leadership*, *37*, 1–11.

Almalki, S. (2016). Integrating quantitative and qualitative data in mixed methods research-challenges and benefits. *Journal of Education and Learning, 5*(3), 288–296. https://doi.org/10.5539/jel.v5n3p288

Alqahtani, F. H. (2017). Developing an information security policy: A case study approach. *Procedia Computer Science*, *124*, 691–697.

https://doi.org/10.1016/j.procs.2017.12.206

Al-Sayyed, R. M. H., Hijawi, W. A., Bashiti, A. M., AlJarah, I., Obeid, N., & Adwan, O. Y. (2019). An investigation of Microsoft Azure and Amazon web services from users' perspectives. *International Journal of Emerging Technologies in Learning*, *14*(10), 217–241. https://doi.org/10.3991/ijet.v14i10.9902

Alshaikh, M., Maynard, S. B., & Ahmad, A. (2021). Applying social marketing to evaluate current security education training and awareness programs in organisations. *Computers & Security*, *100*, 1-19. https://doi.org/10.1016/j.cose.2020.102090

Alves, T., Das, R., Werth, A., & Morris, T. (2018). Virtualization of SCADA testbeds for cybersecurity research: A modular approach. *Computers & Security*, 77, 531–546. https://doi.org/10.1016/j.cose.2018.05.002

Amankwaa, L. (2016). Creating protocols for trustworthiness in qualitative research. *Journal of Cultural Diversity*, *23*(3), 121-127.

Ani, U. D., He, H., & Tiwari, A. (2019). Human factor security: evaluating the cybersecurity capacity of the industrial workforce. *Journal of Systems & Information Technology*, *21*(1), 2. https://doi.org/10.1108/JSIT-02-2018-0028

Arghavani, A., Arghavani, M., Ahmadi, M., & Crane, P. (2018). Attacker-Manager Game Tree (AMGT): A new framework for visualizing and analyzing the interactions between attacker and network security manager. *Computer Networks*, 133, 42–58. https://doi.org/10.1016/j.comnet.2018.01.013

Arundell, F., Mannix, J., Sheehan, A., & Peters, K. (2018). Workplace culture and the practice experience of midwifery students: A meta-synthesis. *Journal of Nursing Management*, *26*(3), 302-313. https://doi.org/10.1111/jonm.12548

Ashibani, Y., & Mahmoud, Q. H. (2017). Cyber physical systems security: Analysis, challenges and solutions. *Computers & Security*, 68, 81–97. https://doi.org//10.1016/j.cose.2017.04.005

Asiamah, N., Mensah, H. K., & Oteng-Abayie, E. F. (2017). General, target, and accessible population: Demystifying the concepts for effective sampling. *Qualitative Report*, *22*(6), 1607–1621.

Atkinson, P. (2017). *Thinking ethnographically.*

Avery, J., & Wallrabenstein, J. R. (2018). Formally modeling deceptive patches using a game-based approach. *Computers & Security*, *75*, 182-190. https://doi.org/10.1016/j.cose.2018.02.009

Bansal, G., Muzatko, S., & Shin, S. I. (2020). Information system security policy noncompliance: the role of situation-specific ethical orientation. *Information Technology & People*, *34*(1), 250–296. https://doi.org/10.1108/ITP-03-2019-0109

Bansal, P. T., Smith, W. K., & Vaara, E. (2018). New ways of seeing through qualitative research. *Academy of Management Journal*, *61*(4), 1189–1195. https://doi.org/10.5465/amj.2018.4004

Barca, D. C. (2017). Information security in digital trunking systems. *Database Systems Journal*, *8*(1), 40–48.

Bauer, S., Bernroider, E. W., & Chudzikowski, K. (2017). Prevention is better than cure! Designing information security awareness programs to overcome users' noncompliance with information security policies in banks. *Computers & Security*, *68,*145-159. https://doi.org/10.1016/j.cose.2017.04.009

Baxter, S., Muir, D., Brereton, L., Allmark, C., Barber, R., Harris, L., Hodges, B., Khan, S., & Baird, W. (2016). Evaluating public involvement in research design and grant development: Using a qualitative document analysis method to analyze an award scheme for researchers. *Research Involvement and Engagement*, *2*, 13-13. https://doi.org/10.1186/s40900-016-0027-x

Bergström, J., van Winsen, R., & Henriqson, E. (2015). On the rationale of resilience in the domain of safety: A literature review. *Reliability Engineering and System Safety*, *141*, 131–141. https://doi.org/10.1016/j.ress.2015.03.008

Bertalanffy, L. (1972). The history and status of general systems theory. Academy of Management Journal, 15, 407-426. https://doi.org/10.2307/255139

Bhamare, D., Zolanvari, M., Erbad, A., Jain, R., Khan, K., & Meskin, N. (2020). Cybersecurity for industrial control systems: A survey. *Computers & Security*, *89*. https://doi.org/10.1016/j.cose.2019.101677

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. https://doi.org/10.1177/1049732316654870

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. https://doi.org/10.1016/j.chb.2018.05.023

Boeren, E. (2018). The methodological underdog: A review of quantitative research in the key adult education journals. *Adult Education Quarterly, 68*(1), 63-79. https://doi.org/10.1177/0741713617739347

Borja, S., Kim, K., Yoon, H., & Hwang, J. (2018). IT governance effectiveness and its influence on innovation product and process. *Journal of Strategic Innovation & Sustainability*, 13(5), 43. https://doi.org/10.23919/picmet.2018.8481752

Boyacı, Ş. D. B., & Guner, M. (2018). The impact of authentic material use on development of the reading comprehension, writing skills and motivation in language course. *International Journal of Instruction*, *11*(2), 351–368. https://doi.org/10.12973/iji.2018.11224a

Brantingham, P. L., & Brantingham, P. L. (1993). Environment, routine and situation: Toward a pattern theory of crime. *Advances in Criminological Theory*, *5*(2), 259-94. https://doi.org/10.4324/9781315128788-12

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

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*. https://doi.org/10.1016/j.cose.2020.101776

Busby, J. S., Green, B., & Hutchison, D. (2017). Analysis of affordance, time, and adaptation in the assessment of industrial control system cybersecurity risk. *Risk Analysis*, *37*(7), 1298–1314. https://doi.org/10.1111/risa.12681

Butavicius, M., Parsons, K., Lillie, M., McCormac, A., Pattinson, M., & Calic, D. (2020).

When believing in technology leads to poor cyber security: Development of a trust in technical controls scale. *Computers & Security*, *98*. https://doi.org/10.1016/j.cose.2020.102020

Cai, H., Toft, E., Hejlesen, J., Oestergaard, C., & Dinesen, B. (2015). Health professionals' user experience of the intelligent bed in patients' homes. *International Journal of Technology Assessment in Health Care, 31*(4)*,* 256-263. https://doi.org/10.1017/s0266462315000380

Callegati, F., Giallorenzo, S., Melis, A., & Prandini, M. (2018). Cloud-of-Things meets Mobility-as-a-Service: An insider threat perspective. *Computers & Security*, 74, 277–295. https://doi.org/10.1016/j.cose.2017.10.006

Caputo, F., Walletzky, L., & Štepánek, P. (2019). Towards a systems thinking based view for the governance of a smart city's ecosystem : A bridge to link smart technologies and big data. *Kybernetes*, *48*(1), 108–123. https://doi.org/10.1108/K-07-2017-0274

Cati, K., Kethuda, O., & Bilgin, Y. (2016). Positioning strategies of universities: An investigation on universities in Istanbul. *Education & Science / Egitim Ve Bilim, 41*(185), 219. https://doi.org/10.15390/EB.2016.2723

Chapman, P. (2021). Defending against insider threats with network security's eighth layer. *Computer Fraud & Security*, *2021*(3), 8–13. https://doi.org/10.1016/S1361-3723(21)00029-4

Chekole, E. G., Chattopadhyay, S., Ochoa, M., Guo, H., & Cheramangalath, U. (2020). CIMA: Compiler-enforced resilience against memory safety attacks in cyber-physical systems. Computers & Security, 94. https://doi.org/10.1016/j.cose.2020.101832

Chen, D. Q., & Liang, H. (2019). Wishful thinking and IT threat avoidance: An extension to the technology threat avoidance theory. *IEEE Transactions on Engineering Management, 66*(4), 552–567. https://doi.org/10.1109/TEM.2018.2835461

Chen, S., Hu, W., & Li, Z. (2019). High-performance data encryption with AES implementation on FPGA. *2019 IEEE 5th Intl Conference on Big Data Security on Cloud (Big Data Security), IEEE Intl Conference on High Performance and Smart Computing (HPSC), and IEEE Intl Conference on Intelligent Data and Security (IDS)*. https://doi.org/10.1109/bigdatasecurity-hpsc-ids.2019.00036

Chen, X., Wu, D., Chen, L., & Teng, J. K. L. (2018). Sanction severity and employees' information security policy compliance: Investigating mediating, moderating, and control variables. *Information & Management*, *55*(8), 1049–1060. https://doi.org/10.1016/j.im.2018.05.011

Cheng, X., Fu, S., & de Vreede, G.-J. (2017). Understanding trust influencing factors in social media communication: A qualitative study. *International Journal of Information Management, 37*, 25–35. https://doi.org/10.1016/j.ijinfomgt.2016.11.009

Cherdantseva, Y., Burnap, P., Blyth, A., Eden, P., Jones, K., Soulsby, H., & Stoddart, K. (2016). A review of cyber security risk assessment methods for SCADA systems. *Computers & Security*, *56*, 1–27. https://doi.org/10.1016/j.cose.2015.09.009

Cherifi, T., & Hamami, L. (2018). A practical implementation of unconditional security for the IEC 60780-5-101 SCADA protocol. *International Journal of Critical Infrastructure Protection*, *20*, 68–84. https://doi.org/10.1016/j.ijcip.2017.12.001

Chia, J., & Chin, J. (2020). An identity based-identification scheme with tight security against active and concurrent adversaries. *IEEE Access*, *8*, 61711–61725. https://doi.org/10.1109/ACCESS.2020.2983750

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. https://doi.org/10.1177/0165551517748288

Chowdhury, N., & Gkioulos, V. (2021). Cyber security training for critical infrastructure protection: A literature review. *Computer Science Review*, *40*. https://doi.org /10.1016/j.cosrev.2021.100361

Civitillo, S., Juang, L. P., Badra, M., & Schachner, M. K. (2019). The interplay between culturally responsive teaching, cultural diversity beliefs, and self-reflection: A multiple case study. *Teaching and Teacher Education, 77*, 341–351. https://doi.org/10.1016/j.tate.2018.11.002

Clark, K. R., & Veale, B. L. (2018). Strategies to enhance data collection and analysis in qualitative research. *Radiologic Technology*, *89*(5), 482CT–485CT.

Clark, R. M., Panguluri, S., Nelson, T. D., & Wyman, R. P. (2017). Protecting drinking water utilities from cyberthreats. *Journal of the American Water Works Association,* 109, 1-29. https://doi.org/10.5942/jawwa.2017.109.0021

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

Cohen, L. E., & Felson, M. (1979). Social Change and Crime Rate Trends: A routine activity approach. *American Sociological Review*, *44*(4), 588–608. https://doi.org/10.2307/2094589

Connelly, L. M. (2016). Understanding research. trustworthiness in qualitative research. *MEDSURG Nursing*, *25*(6), 435–436.

The council of economic advisers. (2018). The cost of malicious cyber activity to the U.S. economy. https://www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf

Crowe, M., Inder, M., & Porter, R. (2015). Conducting qualitative research in mental health: Thematic and content analysis. *Australian & New Zealand Journal of Psychiatry*, *49*, 616-623. https://doi.org/10.1177/0004867415582053

Cuellar, M. J. (2018). School safety strategies and their effects on the occurrence of school-based violence in U.S. high schools: An exploratory study. *Journal of School Violence*, *17*(1), 28–45. https://doi.org/10.1080/15388220.2016.1193742

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

David, S. L., & Hitchcock, J. H. (2018). Understanding Patient Trust in the Athletic Setting through Interviews. *Internet Journal of Allied Health Sciences & Practice*, *16*(2), 1–12.

Demetis, D. S., & Lee, A. S. (2017). Taking the first step with systems theorizing in information systems: A response. *Information and Organization*, *27*(3), 163–170. https://doi.org/10.1016/j.infoandorg.2017.06.003

Dempsey, L., Dowling, M., Larkin, P., & Murphy, K. (2016). Sensitive interviewing in qualitative research. *Research in Nursing & Health*, *39*(6), 480-490. https://doi.org/10.1002/nur21743

Deng, J. (1982). Grey systems control. *Systems & Control Letters*, *1*, 288-294. https://doi.org/10.1016/S0167-6911(82)80025-X

Diesch, R., Pfaff, M., & Krcmar, H. (2020). A comprehensive model of information security factors for decision-makers. *Computers & Security*, *92*. https://doi.org/10.1016/j.cose.2020.101747

Dikko, M. (2016). Establishing construct validity and reliability: pilot testing of a qualitative interview for research in Takaful (Islamic insurance). *Qualitative Report*, *21*(3), 521–528.

Di Mauro, C., Fratocchi, L., Orzes, G., & Sartor, M. (2018). Offshoring and backshoring: A multiple case study analysis. *Journal of Purchasing and Supply Management, 24*(2), 108-134. https://doi.org/10.1016/j.pursup.2017.07.003

Drack, M., & Pouvreau, D. (2015). On the history of Ludwig von Bertalanffy's "General Systemology," and on its relationship to cybernetics – part III: convergences and divergences. International Journal of General Systems, 44(5), 523–571. https://doi.org/10.1080/03081079.2014.1000642

Dreier, J., Puys, M., Potet, M.-L., Lafourcade, P., & Roch, J.-L. (2019). Formally and practically verifying flow properties in industrial systems. *Computers & Security.* https://doi.org/10.1016/j.cose.2018.09.018

Dube, F. N., & Uys, L. R. (2015). Primary health care nurses' management practices of common mental health conditions in KwaZulu-Natal, South Africa. *Curationis*, *38*(1), e1–e10. https://doi.org/10.4102/curationis.v38i1.1168

Durkota, K., Lisy, V., Kiekintveld, C., Bosansky, B., & Pechoucek, M. (2016). Case studies of network defense with attack graph games. *IEEE Intelligent Systems*, *31*(5), 24-30. https://doi.org/10.1109/MIS.2016.74

Elhady, A. M., El-bakry, H. M., & Abou Elfetouh, A. (2019). Comprehensive risk identification model for SCADA systems. *Security & Communication Networks*, 1–24. https://doi.org/10.1155/2019/3914283

Elifoglu, I. H., Abel, I., & Taşseven, Ö. (2018). Minimizing insider threat risk with behavioral monitoring. *Review of Business*, *38*(2), 61–73.

Elkatawneh, H. H. (2016). The five qualitative approaches: Problem, purpose, and questions/the role of theory in the five qualitative approaches/comparative case study. *SSRN Electronic Journal*, 1-18. https://doi.org/10.2139/ssrn.2761327

Emmel, N. (2015). Themes, variables, and the limits to calculating sample size in qualitative research: a response to Fugard and Potts. *International Journal of Social Research Methodology*, *18*(6), 685–686. https://doi.org/10.1080/13645579.2015.1005457

Feng, B., Li, Q., Ji, Y., Guo, D., & Meng, X. (2019). Stopping the cyberattack in the early stage: Assessing the security risks of social network users. *Security and*

Communication Networks. https://doi.org/10.1155/2019/3053418

Fernández, D. M., & Wagner, S. (2016). Case studies in industry: What we have learnt. *In Proceedings of the 4th International Workshop on Conducting Empirical Studies in Industry* (CESI '16). https://doi.org/10.1145/2896839.2896844

Fink, G., Edgar, T., Rice, T., MacDonald, D., & Crawford, C. (2017). Security and privacy in cyber-physical systems. In Intelligent Data-Centric Systems (Editors.), *Cyber-physical systems* (pp. 129-141). https://doi.org/10.1016/b978-0-12-803801-7.00009-2

Forde, E. S. (2017). *Security Strategies for Hosting Sensitive Information in the Commercial Cloud*.

Gagnon, M., Jacob, J. D., & McCabe, J. (2015). Locating the qualitative interview: reflecting on space and place in nursing research. *Journal of Research in Nursing*, *3*, 203. https://doi.org/10.1177/1744987114536571

Galvin, R. (2015). How many interviews are enough? Do qualitative interviews in building energy consumption research produce reliable knowledge? *Journal of Building Engineering*, *1*, 2-12. https://doi.org/10.1016/j.jobe.2014.12.001

Gaurav, D., Sidhu, J., & Mohana, R. (2020). Access Management of user and cyber-physical device in DBaaS according to Indian IT laws using blockchain. *Scalable Computing: Practice & Experience*, *21*(3), 407–424. https://doi.org/10.12694/scpe.v21i3.1737

Gcaza, N., von Solms, R., Grobler, M. M., & van Vuuren, J. J. (2017). A general morphological analysis: delineating a cyber-security culture. *Information &*

Computer Security, *25*(3), 259–278. https://doi.org/10.1108/ICS-12-2015-0046

Genge, B., Haller, P., & Duka, A.-V. (2019). Engineering security-aware control applications for data authentication in smart industrial cyber–physical systems. *Future Generation Computer Systems*, *91*, 206–222. https://doi.org/ 10.1016/j.future.2018.09.001

Gergen, K. J., Josselson, R., & Freeman, M. (2015). The promises of qualitative inquiry. *American Psychologist, 70*, 1. https://doi.org/10.1037/a0038597

Ghaleb, A., Zhioua, S., & Almulhem, A. (2018). On PLC network security. *International Journal of Critical Infrastructure Protection*, *22*, 62–69. https://doi.org/10.1016/j.ijcip.2018.05.004

Ghosh, S., & Sampalli, S. (2019). A survey of security in SCADA networks: Current issues and future challenges. *IEEE Access, 7*, 135812–135831. https://doi.org/10.1109/Access.2019.2926441

Goh, T. (2020). Making cybersecurity training a priority. *Chemical Engineering*, *127*(2), 32–37.

Gopalakrishna-Remani, V., Jones, R. P., & Camp, K. M. (2018). Levels of EMR adoption in US hospitals: An empirical examination of absorptive capacity, institutional pressures, top management beliefs, and participation. *Information Systems Frontiers,* 1-20. https://doi.org/10.1007/s10796-018-9836-9

Grabowski, M., & Roberts, K. H. (2019). Reliability seeking virtual organizations: Challenges for high reliability organizations and resilience engineering. *Safety Science*, *117*, 512–522. https://doi.org/10.1016/j.ssci.2016.02.016

Grassegger, T., & Nedbal, D. (2021). The role of employees' information security awareness on the intention to resist social engineering. *Procedia Computer Science*, *181*, 59–66. https://doi.org/10.1016/j.procs.2021.01.103

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

Gregory, R. W., Kaganer, E., Henfridsson, O., & Ruch, T. J. (2018). IT consumerization and the transformation of IT governance. *MIS Quarterly*, 42(4), 1225-1253. https://doi.org/10.25300/MISQ/2018/13703

Gunasekaran, V., Dey, S., Chakrawarty, A., Chatterjee, P., Sati, H. C., Dwivedi, S. N., & Dey, A. B. (2018). Raised serum cystatin C can be a potential biomarker of frailty detected by cumulative deficit model. *Aging Medicine*, *1*(2), 149–153.

Guo, Y., & Zhang, Z. (2018). LPSE: Lightweight password-strength estimation for password meters. *Computers & Security, 73*, 507–518. https://doi.org/10.1016/j.cose.2017.07.012

Guo, Y., Zhang, Z., & Guo, Y. (2019). Optiwords: A new password policy for creating memorable and strong passwords. *Computers & Security*, *85*, 423–435. https://doi.org /10.1016/j.cose.2019.05.015

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.

Harlow, C. (2018, August 1). Securing Open SCADA Systems for Pipeline Operations. *Pipeline & Gas Journal*, *245*(8), 64.

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

Hartnell, C. A., Ou, A. Y., Kinicki, A. J., Choi, D., & Karam, E. P. (2019). A meta-analytic test of organizational culture's association with elements of an organization's system and its relative predictive validity on organizational outcomes. *Journal of Applied Psychology*. https://doi.org/10.1037/apl0000380.supp.

Hayhurst, C. (2018). Sewing up solutions: The role of software patch management in effective cybersecurity. *Biomedical Instrumentation & Technology*, *52*(2), 92-102. https://doi.org /10.2345/0899-8205-52.2.92

He, W., Ash, I., Anwar, M., Li, L., Yuan, X., Xu, L., & Tian, X. (2020). Improving employees' intellectual capacity for cybersecurity through evidence-based malware training. *Journal of Intellectual Capital*, *21*(2), 203–213. https://doi.org /10.1108/JIC-05-2019-0112

He, W., & Zhang, Z. (2019). Enterprise cybersecurity training and awareness programs: Recommendations for success. *Journal of Organizational Computing and Electronic Commerce*, 1-9. https://doi.org/10.1080/10919392.2019.1611528

He, Y., & Johnson, C. (2017). Challenges of information security incident learning: An industrial case study in a Chinese healthcare organization. *Informatics for Health & Social Care*, *42*(4), 393–408. https://doi.org/10.1080/17538157.2016.1255629

Heydon, G., & Powell, A. (2018). Written-response interview protocols: an innovative approach to confidential reporting and victim interviewing in sexual assault investigations. *Policing & Society*, *28*(6), 631–646. https://doi.org/10.1080/10439463.2016.1187146

Homoliak, I., Toffalini, F., Guarnizo, J., Elovici, Y., & Ochoa, M. (2019). Insight into insiders and IT. *ACM Computing Surveys*, *52*(2), 1–40. https://doi.org/10.1145/3303771

Huda, S., Yearwood, J., Hassan, M. M., & Almogren, A. (2018). Securing the operations in SCADA-IoT platform based industrial control system using ensemble of deep belief networks. *Applied Soft Computing*, *71*, 66–77. https://doi.org/10.1016/j.asoc.2018.06.017

Hughes, H. P. N., Clegg, C. W., Bolton, L. E., & Machon, L. C. (2017). Systems scenarios: a tool for facilitating the socio-technical design of work systems. *Ergonomics*, *60*(10), 1319–1335. https://doi.org/10.1080/00140139.2017.1288272

Huygh, T., & De Haes, S. (2019). Investigating IT Governance through the Viable System Model. *Information Systems Management*, *36*(2), 168–192. https://doi.org/10.1080/10580530.2019.1589672

Iivari, N. (2018). Using member checking in interpretive research practice: A hermeneutic analysis of informants' interpretation of their organizational realities. *Information Technology & People*, (1), 111. https://doi.org/10.1108/ITP-07-2016-0168

Indu, I., Anand, P. M. R., & Bhaskar, V. (2018). Identity and access management in cloud environment: Mechanisms and challenges. *Engineering Science and Technology, an International Journal*, *21*(4), 574–588. https://doi.org/10.1016/j.jestch.2018.05.010

Ivankova, N., & Wingo, N. (2018). Applying mixed methods in action research: Methodological potentials and advantages. *American Behavioral Scientist*, *62*(7), 978–997. https://doi.org/10.1177/0002764218772673

Jacobs, J., Romanosky, S., Adjerid, I., & Baker, W. (2020). Improving vulnerability remediation through better exploit prediction. *Journal of Cybersecurity, 5(1)*, https://doi.org/10.1093/cybsec/tyaa015

Jae-Myeong, L., & Sugwon, H. (2020). Keeping host sanity for security of the SCADA systems. *IEEE Access*, *8*, 62954–62968. https://doi.org/10.1109/Access.2020.2983179

Jamison, J., Sutton, S., Mant, J., & De Simoni, A. (2018). Online stroke forum as source of data for qualitative research: insights from a comparison with patients' interviews. *BMJ Open, 8*(3). https://doi.org/10.1136/bmjopen-2017-020133

Jarvis, J. E., & Williams, I. A. (2017). A case study exploration of strategies to improve first-line supervisor problem-solving abilities in the retail supermarket industry. *International Journal of Applied Management and Technology,* 16(1), 86–110. https://doi.org/10.5590/ijamt.2017.16.1.06

Johnson, M., O’Hara, R., Hirst, E., Weyman, A., Turner, J., Mason, S., Quinn, T., Shewan, J., & Siriwardena, A. N. (2017). Multiple triangulation and collaborative research using qualitative methods to explore decision making in pre-hospital emergency care. *BMC Medical Research Methodology*, *17*(1), 1-11. https://doi.org/10.1186/s12874-017-0290-z

Johnson, O. (2019). General system theory and the use of process mining to improve care pathways. *Studies in Health Technology and Informatics*, *263*, 11–22. https://doi.org /10.3233/SHTI190107

Joslin, R., & Muller, R. (2016). Identifying interesting project phenomena using philosophical and methodological triangulation. *International Journal of Project Management*, 34, 1043-1056. https://doi.org/10.1016/j.ijproman.2016.05.005

Kaefer, F., Roper, J., & Sinha, P. (2015). A software-assisted qualitative content analysis of news articles: Example and reflections. *Forum Qualitative Sozialforschung*, *16*(2), 1-20. https://doi.org/10.17169/fqs-16.2.2123

Kalech, M. (2019). Cyber-attack detection in SCADA systems using temporal pattern recognition techniques. *Computers & Security*, 84, 225–238. https://doi.org/10.1016/j.cose.2019.03.007

Kaley, A., Hatton, C., & Milligan, C. (2019). More than words: The use of video in ethnographic research with people with intellectual disabilities. *Qualitative Health Research*, *29*(7), 931–943. https://doi.org/10.1177/1049732318811704

Kallio, H., Pietila, A. M., Johnson, M., & Kangasniemi, M. (2016). Systematic methodological review: Developing a framework for a qualitative semi-structured interview guide. *Journal of Advanced Nursing, 72*(12), 2954-2965. https://doi.org/10.1111/jan.13031

Katrakazas, P., Pastiadis, K., Bibas, A., & Koutsouris, D. (2020). A general systems theory approach in public hearing health: Lessons learned from a systematic review of general systems theory in healthcare. *IEEE Access*, 8, 53018-53033. https://doi.org/10.1109/ACCESS.2020.2981160

Kim, H. L., Hovav, A., & Han, J. (2020). Protecting intellectual property from insider threats: A management information security intelligence perspective. *Journal of Intellectual Capital*, *21*(2), 181–202. https://doi.org/10.1108/JIC-05-2019-0096

Kim, S.-J., Cho, D.-E., & Yeo, S.-S. (2014). Secure model against APT in m-connected SCADA network. *International Journal of Distributed Sensor Networks*. https://doi.org/10.1155/2014/594652

King, K. M., Pullmann, M. D., Lyon, A. R., Dorsey, S., & Lewis, C. C. (2019). Using implementation science to close the gap between the optimal and typical practice of quantitative methods in clinical science. *Journal of Abnormal Psychology*, *128*(6), 547–562. https://doi.org/10.1037/abn0000417

Kong, S. Y., Yaacob, N. M., & Ariffin, A. R. M. (2018). Constructing a mixed methods research design: Exploration of an architectural intervention. *Journal of Mixed Methods Research, 12*(2), 148–165. https://doi.org/10.1177/1558689816651807

Kongnso, F. (2015). *Best practices to minimize data security breaches for increased business performance* (Doctoral dissertation).

Korstjens, I., & Moser, A. (2018). Series: Practical guidance to qualitative research. Part 4: Trustworthiness and publishing. *European Journal of General Practice, 24*(1), 120-124. https://doi.org/10.1080/13814788.2017.1375092

Kowalski, C. J., Hutchinson, R. J., & Mrdjenovich, A. J. (2017). The ethics of clinical care and the ethics of clinical research: Yin and Yang. *Journal of Medicine & Philosophy, 42*(1), 7–32. https://doi.org/10.1093/jmp/jhw032

Kristiyanto, Y., & Ernastuti, E. (2020). Analysis of deauthentication attack on IEEE 802.11 Connectivity based on IoT technology using external penetration test. *CommIT Journal*, *14*(1), 45–51. https://doi.org /10.21512/commit.v14i1.6337

Kruth, J. G. (2015). Five qualitative research approaches and their applications in parapsychology 1. *The Journal of Parapsychology*, *79*(2), 219-233.

Kunz, M., Puchta, A., Groll, S., Fuchs, L., & Pernul, G. (2019). Attribute quality management for dynamic identity and access management. *Journal of Information Security and Applications*, *44*, 64–79. https://doi.org/10.1016/j.jisa.2018.11.004

Kure, H. I., Islam, S., & Abdur Razzaque, M. (2018). An integrated cyber security risk management approach for a cyber-physical system. *Applied Sciences*, (6), 898. https://doi.org/10.3390/app8060898

Laage, T., Loewy, J. W., Menon, S., Miller, E. R., Pulkstenis, E., Kan-Dobrosky, N., & Coffey, C. (2017). Ethical considerations in adaptive design clinical trials. *Therapeutic Innovation & Regulatory Science, 51*(2), 190–199. https://doi.org/10.1177/2168479016667766

Lai, J., Mu, Y., Guo, F., Jiang, P., & Susilo, W. (2018). Privacy-enhanced attribute-based private information retrieval. *Information Sciences*, *454–455*, 275–291. https://doi.org/10.1016/j.ins.2018.04.084

Lal, S., Taleb, T., & Dutta, A. (2017). NFV: Security threats and best practices. *IEEE Communications Magazine*, *55*(8), 211-217. https://doi.org/10.1109/MCOM.2017.1600899

Lasrado, F., & Uzbeck, C. (2017). The excellence quest: a study of business excellence award-winning organizations in UAE. *Benchmarking: An International Journal*, *24*(3), 716-734. https://doi.org/10.1108/BIJ-06-2016-0098

Lee, H., Lim, D., Kim, H., Zo, H., & Cigaek, A. P. (2015). Compensation paradox: the influence of monetary rewards on user behaviour. *Behaviour & Information Technology*, *34*(1), 45-56. https://doi.org/10.1080/0144929X.2013.805244

Lee, J., & Hong, S. (2020). Keeping host sanity for security of the SCADA systems. *IEEE Access, 8*, 62954–62968. https://doi.org/10.1109/Access.2020.2983179

Leedy, P. D., & Ormrod, J. E. (2015). *Practical research: Planning and design* (11th ed.). New York, NY.

Leszczyna, R. (2018). A review of standards with cybersecurity requirements for smart grid. *Computers & Security.* https://doi.org/10.1016/j.cose.2018.03.011

Leung, L. (2015). Validity, reliability, and generalizability in research. *Journal of Family Medicine & Primary Care, 4*, 324–327. https://doi.org/10.4103/2249-4863.161306

Levitt, H. M., Bamberg, M., Creswell, J. W., Frost, D. M., Josselson, R., & Suárez-Orozco, C. (2018). Journal article reporting standards for qualitative primary, qualitative meta-analytic, and mixed methods research in psychology: The APA publications and communications board task force report. *American Psychologist, 73*(1), 26–46. https://doi.org/10.1037/amp0000151

Li, D., Guo, H., Zhou, J., Zhou, L., & Wong, J. W. (2019). SCADAWall: A CPI-enabled firewall model for SCADA security. *Computers & Security*, *80*, 134–154. https://doi.org/10.1016/j.cose.2018.10.002

Li, J., Greenwood, D., & Kassem, M. (2019). Blockchain in the built environment and construction industry: A systematic review, conceptual models and practical use cases. *Automation in Construction*, *102*, 288–307. https://doi.org/10.1016/j.autcon.2019.02.005

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. https://doi.org/10.1016/j.ijinfomgt.2018.10.017

Li, W., Xie, L., Deng, Z., & Wang, Z. (2016). False sequential logic attack on SCADA system and its physical impact analysis. *Computers & Security*, *58*, 149–159. https://doi.org/10.1016/j.cose.2016.01.001

Liang, H., & Xue, Y. (2009). Avoidance of information technology threats: A theoretical perspective. MIS Quarterly, 33(1), 71-90

Lollai, S. A. (2017). Quality systems. A thermodynamics-related interpretive model. *Entropy*, *19*(8), 418. https://doi.org/10.3390/e19080418

Loukaka, A., & Rahman, S. (2017). Discovering new cyber protection approaches from a security professional prospective. *International Journal of Computer Networks &*

Communications, *9*(4). https://doi.org/10.5121/ijcnc.2017.9402

Low, J. K., Crawford, K., Manias, E., & Williams, A. (2016). A compilation of consumers' stories: The development of a video to enhance medication adherence in newly transplanted kidney recipients. *Journal of Advanced Nursing. 72*(4), 813-824. https://doi.org/10.1111/jan.12886

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. https://doi.org/10.1177/1525822X17749386

Lucas, T. K. (2019). Measuring knowledge sharing behaviour among software development teams. *South African Journal of Information Management*, *21*(1), e1–e7. https://doi.org/10.4102/sajim.v21i1.1076

Maglaras, L. A., Jiang, J., & Cruz, T. J. (2016). Combining ensemble methods and social network metrics for improving accuracy of OCSVM on intrusion detection in SCADA systems. *Journal of Information Security and Applications*, *30*, 15–26. https://doi.org//10.1016/j.jisa.2016.04.002

Maher, C., Hadfield, M., Hutchings, M., & de Eyto, A. (2018). Ensuring rigor in qualitative data analysis: A design research approach to coding combining NVivo with traditional material methods. *International Journal of Qualitative Methods*. *17*, 1-13. https://doi.org/10.1177/1609406918786362

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. https://doi.org/10.1016/j.cose.2020.101901

Malatji, M., Marnewick, A., & von Solms, S. (2020). Validation of a socio-technical management process for optimising cybersecurity practices. *Computers & Security*, *95*. https://doi.org/10.1016/j.cose.2020.101846

Malecic, A. (2017). Footprints of general systems theory. *Systems Research & Behavioral Science*, *34*(5), 631–636. https://doi.org/10.1002/sres.2484

Mandal, P. C. (2018). Trustworthiness in qualitative content analysis. *International Journal of Advanced Research and Development*, *3*(2), 479-485.

Mar, S. (2019, April 1). The single point of failure: The death of a CEO highlights the risks of only one person controlling access to corporate data. *Internal Auditor*, *76*(2), 16-17.

Maramwidze-Merrison, E. (2016). Innovative methodologies in qualitative research: Social media window for accessing organisational elites for interviews. *Electronic Journal of Business Research Methods*, *14*(2), 157–167.

Markovic-Petrovic, J. D., Stojanovic, M. D., & Bostjancic Rakas, S. V. (2019). A fuzzy AHP approach for security risk assessment in SCADA networks. *Advances in Electrical and Computer Engineering*, *3*, 69. https://doi.org/10.4316/AECE.2019.03008

Marshall, C., & Rossman, G. B. (2016). Designing qualitative research, Sixth Edition*. Canadian Journal of Sociology, 40*(3), 399.

Martín-Liras, L., Prada, M. A., Fuertes, J. J., Morán, A., Alonso, S., & Domínguez, M. (2017). Comparative analysis of the security of configuration protocols for industrial control devices. *International Journal of Critical Infrastructure*

Protection, *19*, 4–15. https://doi.org/10.1016/j.ijcip.2017.10.001

Mazzei, M., Ketchen, D. J., & Shook, C. (2017). Understanding strategic entrepreneurship: a "theoretical toolbox" approach. *International Entrepreneurship and Management Journal*, 13(2), 631–663. https://doi.org/10.1007/s11365-016-0419-2

McCusker, K., & Gunaydin, S. (2015). Research using qualitative, quantitative or mixed methods and choice based on the research. *Perfusion, 30*(7), 537–542. https://doi.org/10.1177/0267659114559116

Midi, D., Sultana, S., & Bertino, E. (2016). A system for response and prevention of security incidents in wireless sensor networks. *ACM Transactions on Sensor Networks*, *13*(1), 1–38. https://doi.org/10.1145/2996195

Mihalos, M. G., Nalmpantis, S. I., & Ovaliadis, K. (2019). Design and implementation of firewall security policies using Linux iptables. *Journal of Engineering Science & Technology Review*, *12*(1), 80-86. https://doi.org/10.25103/jestr.121.09

Mohamed, N. L. (2017). Review on SCADA cybersecurity for critical infrastructures. *Journal of Computer Science & Control Systems*, *10*(1), 15–18.

Molin, E., Meeuwisse, K., Pieters, W., & Chorus, C. (2018). Secure or usable computers? Revealing employees' perceptions and trade-offs by means of a discrete choice experiment. *Computers & Security*, *77*, 65–78. https://doi.org/10.1016/j.cose.2018.03.003

Morse, J. M. (2015). Critical analysis of strategies for determining rigor in qualitative inquiry. *Qualitative Health Research*, *25*(9), 1212-1222.

https://doi.org/10.1177/1049732315588501

Muratoğlu, O., Okul, S., Aydm, M. A., & Bilge, H. Ş. (2018). Review on cyber risks relating to security management in smart cars. *2018 3rd International Conference on Computer Science and Engineering (UBMK)*, 406-409. https://doi.org/10.1109/UBMK.2018.8566569

Murillo, P. A. F., Gaur, V., Giraldo, J., Cardenas, A. A., & Rueda, S. J. (2018). Leveraging software-defined networking for incident response in industrial control systems. *IEEE Software, 35*(1), 44–50. https://doi.org/10.1109/MS.2017.4541054

Myers, D., Suriadi, S., Radke, K., & Foo, E. (2018). Anomaly detection for industrial control systems using process mining. Computers & Security, 78, 103–125. https://doi.org/10.1016/j.cose.2018.06.002

Nazir, S., Patel, S., & Patel, D. (2017). Assessing and augmenting SCADA cyber security: A survey of techniques. *Computers & Security*, 70, 436–454. https://doi.org/10.1016/j.cose.2017.06.010

Nebeker, C., Lagare, T., Takemoto, M., Lewars, B., Crist, K., Bloss, C. S., & Kerr, J. (2016). Engaging research participants to inform the ethical conduct of mobile imaging, pervasive sensing, and location tracking research. *Translational Behavioral Medicine*, *6*(4), 577-586. https://doi.org/10.1007/s13142-016-0426-4

Nelson, A. M. (2016). Methodology for examining attributes of African Americans in the department of defense senior executive service corp. *Journal of Economic Development, Management, IT, Finance, and Marketing,* 8(1), 48-68.

Niemimaa, M., & Niemimaa, E. (2019). Abductive innovations in information security policy development: an ethnographic study. *European Journal of Information Systems*, *28*(5), 566–589. https://doi.org /10.1080/0960085X.2019.1624141

Oakley, J. G. (2019). The state of modern offensive security. *Professional Red Teaming*, 29-41. https://doi.org/10.1007/978-1-4842-4309-1_3.

Ofori-Duodu, M. S. (2019). *Exploring Data Security Management Strategies for Preventing Data Breaches*.

Orange, A. (2016). Encouraging reflexive practices in doctoral students through research journals. *Qualitative Report, 21*(12), 2176-2190.

Paananen, H., Lapke, M., & Siponen, M. (2020). State of the art in information security policy development. *Computers & Security*, *88*. https://doi.org/10.1016/j.cose.2019.101608

Padilla, V. S., & Freire, F. F. (2019). A contingency plan framework for cyber-attacks. *Journal of Information Systems Engineering & Management, 4*(2), em0098. https://doi.org/10.29333/jisem/5898

Palanisamy, R., Norman, A. A., & Kiah, M. L. M. (2020). Compliance with bring your own device security policies in organizations: A systematic literature review. *Computers & Security*, *98*. https://doi.org/10.1016/j.cose.2020.101998

Palinkas, L. A., Horwitz, S. M., Green, C. A., Wisdom, J. P., Duan, N., & Hoagwood, K. (2015). Purposeful sampling for qualitative data collection and analysis in mixed method implementation research. *Administration and Policy in Mental Health and Mental Health Services Research*, *42*(5), 533-544.

https://doi.org/10.1007/s10488-013-0528-y

Pascual-García, A. (2018). A constructive approach to the epistemological problem of emergence in complex systems. *PLoS ONE*, *13*(10), 1–31. https://doi.org/10.1371/journal.pone.0206489

Patel, M. (2020). *Demilitarized zone: An exceptional layer of network security to mitigate DDoS attack* [Doctoral dissertation, University of Windsor, Canada]. University of Windsor Digital Archive. https://scholar.uwindsor.ca/cgi/viewcontent.cgi?article=9311&context=etd

Peticca-Harris, A., deGama, N., & Elias, S. (2016). A dynamic process model for finding informants and gaining access in qualitative research. *Organizational Research Methods, 19*(3), 376–401. https://doi.org/10.1177/1094428116629218

Phipps, W. D. (2019). Toward an integrative approach: Refiguring essential developments in family therapy. *Journal of Family Psychotherapy*, *30*(2), 116–140. https://doi.org/10.1080/08975353.2019.1601447

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

Pol, M. V. J. (2019). Identity and access management tools. *International Journal of Trend in Scientific Research and Development*, *3(*4*)*, 796–798. https://doi.org/10.31142/ijtsrd23935

Qassim, Q. S., Jamil, N., Daud, M., Patel, A., & Ja'affar, N. (2019). A review of security assessment methodologies in industrial control systems. *Information & Computer*

Security, *27*(1), 47–61. https://doi.org/10.1108/ICS-04-2018-0048

Qian, J., Hua, C., Guan, X., Xin, T., & Zhang, L. (2019). A trusted-ID referenced key scheme for securing SCADA communication in iron and steel plants. *Access, IEEE*, *7*, 46947–46958. https://doi.org/10.1109/Access.2019.2909011

Radoglou-Grammatikis, P. I., & Sarigiannidis, P. G. (2019). Securing the smart grid: A comprehensive compilation of intrusion detection and prevention systems. *IEEE Access, 7*, 46595–46620. https://doi.org/10.1109/Access.2019.2909807

Rakas, S. V. B., Stojanovic, M. D., & Markovic-Petrovic, J. D. (2020). A review of research work on network-based SCADA intrusion detection systems. IEEE Access, 8, 93083–93108. https://doi.org/10.1109/ACCESS.2020.2994961

Ranney, M. L., Meisel, Z. F., Choo, E. K., Garro, A. C., Sasson, C., & Morrow, K. (2015). Interview-based qualitative research in emergency care part II: Data collection, analysis and results reporting. *Academic Emergency Medicine*. *22*(9), 1103-1112. https://doi.org/10.1111/acem.12735

Rapp, A., Gabler, C., & Ogilvie, J. (2020). A holistic perspective of sales research: areas of consideration to develop more comprehensive conceptual and empirical frameworks. *Journal of Personal Selling & Sales Management*, *40*(4), 227–233. https://doi.org /10.1080/08853134.2020.1823229

Renz, S. M., Carrington, J. M., & Badger, T. A. (2018). Two strategies for qualitative content analysis: An intramethod approach to triangulation. *Qualitative Health Research, 28*(5), 824-831. https://doi.org/10.1177/1049732317753586

Richardson, J. A. (2018). The discovery of cumulative knowledge: Strategies for designing and communicating qualitative research. *Accounting, Auditing & Accountability Journal*, 31(2), 563-585. https://doi.org/10.1108/aaaj-08-2014-1808

Ridder, H.-G. (2017). The theory contribution of case study research designs. *Business Research, 10*(2), 281–305. https://doi.org/10.1007/s40685-017-0045-z

Rimando, M., Brace, A., Namageyo-Funa, A., Parr, T. L., Sealy, D.-A., Davis, T. L., Martinez, L. M., & Christiana, R. W. (2015). Data collection challenges and recommendations for early career researchers. *Qualitative Report, 20*(12), 2025-2036.

Rivas-Asanza, W., Celleri-Pacheco, J., Andrade-Garda, J., García-Vázquez, R., Mato-Abad, V., Rodríguez-Yáñez, S., & Suárez-Garaboa, S. (2018). Environmental sustainability in information technologies governance. *Sustainability*, 10(12), 4792. https://doi.org/10.3390/su10124792

Roberts, L., & Allen, P. (2015). Exploring ethical issues associated with using online surveys in educational research. *Educational Research and Evaluation, 21*(2), 95-108. https://doi.org/10.1080/13803611.2015.1024421

Rochlin, G. I. (1996). Reliable organizations: present research and future directions. *Journal of Contingencies & Crisis Management*, *4*(2), 55. https://doi.org/10.1111/j.1468-5973.1996.tb00077.x

Rochlin, G. I., La Porte, T. R., & Roberts, K. H. (1998). The self-designing high-reliability organization. *Naval War College Review.* 51(3), 1-17.

Rodofile, N. R., Radke, K., & Foo, E. (2019). Extending the cyber-attack landscape for scada-based critical infrastructure. *International Journal on Critical Infrastructure Protection*, 25, 14–35. https://doi.org/10.1016/j.ijcip.2019.01.002

Rong, L., Bing, T., Yan, L., & Yansheng, Q. (2019). Information security evaluation based on artificial neural network. *International Journal of Performability Engineering*, *11*, 2908–2915. https://doi.org /10.23940/ijpe.19.11.p9.29082915

Rosa, L., Freitas, M., Mazo, S., Monteiro, E., Cruz, T., & Simoes, P. (2019). A comprehensive security analysis of a SCADA protocol: From OSINT to mitigation. *IEEE Access, 7*, 42156–42168. https://doi.org/10.1109/Access.2019.2906926

Rostami, E., Karlsson, F., & Gao, S. (2020). Requirements for computerized tools to design information security policies. *Computers & Security*, *99*. https://doi.org/10.1016/j.cose.2020.102063

Rousseau, D. (2017). Strategies for discovering scientific systems principles. *Systems Research & Behavioral Science*, *34*(5), 527–536. https://doi.org/10.1002/sres.2488

Safa, N. S., Maple, C., Watson, T., & Von Solms, R. (2018). Motivation and opportunity based model to reduce information security insider threats in organisations. *Journal Of Information Security And Applications*, *40*, 247–257. https://doi.org/10.1016/j.jisa.2017.11.001

Sallos, M. P., Garcia-Perez, A., Bedford, D., & Orlando, B. (2019). Strategy and organisational cybersecurity: a knowledge-problem perspective. *Journal of Intellectual Capital*, *20*(4), 581–597. https://doi.org /10.1108/JIC-03-2019-0041

Sarginson, N. (2020). Securing your remote workforce against new phishing attacks. *Computer Fraud & Security*, *2020*(9), 9–12. https://doi.org/10.1016/S1361-3723(20)30096-8

Sarstedt, M., Bengart, P., Shaltoni, A. M., & Lehmann, S. (2017). The use of sampling methods in advertising research: A gap between theory and practice. *International Journal of Advertising*, 1-14. https://doi.org/10.1080/02650487.2017.1348329

Saunders, F. C., Gale, A. W., & Sherry, A. H. (2016). Responding to project uncertainty: Evidence for high reliability practices in large-scale safety–critical projects. *International Journal of Project Management*, *34*(7), 1252–1265. https://doi.org/10.1016/j.ijproman.2016.06.008

Sawyer, B. D., & Hancock, P. A. (2018). Hacking the human: The prevalence paradox in cybersecurity. *Human Factors*, 60(5), 597–609. https://doi.org/10.1177/0018720818780472

Schlegel, R., Hristova, A., & Obermeier, S. (2015). A framework for incident response in industrial control systems. *2015 12th International Joint Conference on E-Business and Telecommunications (ICETE), 04*, 178–185.

Schrimpf, A., Drechsler, A., & Dagianis, K. (2021). Assessing identity and access management process maturity: First insights from the german financial sector. *Information Systems Management*, *38*(2), 94–115. https://doi.org/10.1080/10580530.2020.1738601

Schultze, U. (2017). What kind of world do we want to help make with our theories? *Information & Organization*, *27*(1), 60–66.

https://doi.org/10.1016/j.infoandorg.2017.01.002

Schuster, S., van den Berg, M., Larrucea, X., Slewe, T., & Ide-Kostic, P. (2017). Mass surveillance and technological policy options: Improving security of private communications. *Computer Standards & Interfaces*, *50*, 76–82. https://doi.org/10.1016/j.csi.2016.09.011

Scrutton, R., & Beames, S. (2015). Measuring the unmeasurable: Upholding rigor in quantitative studies of personal and social development in outdoor adventure education. *Journal of Experiential Education*. 38(1), 8-25. https://doi.org/10.1177/1053825913514730.

Shahzad, A., Lee, M., Kim, S., Kim, K., Choi, J., Cho, Y., & Lee, K. (2016). Design and development of layered security: Future enhancements and directions in transmission. *Sensors (14248220)*, *16*(1), 37. https://doi.org/10.3390/s16010037

Sharma, S., & Warkentin, M. (2019). Do I really belong?: Impact of employment status on information security policy compliance. *Computers & Security*, *87*. https://doi.org/10.1016/j.cose.2018.09.005

Shitharth, S., & Winston, P. D. (2017). An enhanced optimization based algorithm for intrusion detection in SCADA network. *Computers & Security*, *70*, 16–26. https://doi.org/10.1016/j.cose.2017.04.012

Shlomo, A., Kalech, M., & Moskovitch, R. (2021). Temporal pattern-based malicious activity detection in SCADA systems. *Computers & Security*, *102*. https://doi.org/10.1016/j.cose.2020.102153

Shoemaker, D., Davidson, D., & Conklin, A. (2017). Toward a discipline of cyber security: Some parallels with the development of software engineering education. *EDPACS*, *56*(5-6), 12-20. https://doi.org/10.1080/07366981.2017.1404867

Sifeng, L., Tao, L., Xie, N., & Yang, Y. (2016). On the new model system and framework of grey system theory. *Journal of Grey System*, *28*, 1-15. https://doi.org/10.1109/GSIS.2015.7301810

Silva, A., Silva, K., Rocha, A., & Queiroz, F. (2019). Calculating the trust of providers through the construction weighted Sec-SLA. *Future Generation Computer Systems*, *97*, 873–886. https://doi.org/10.1016/j.future.2019.02.034

Simola, S. (2018). Fostering collective growth and vitality following acts of moral courage: A general system, relational psychodynamic perspective. *Journal of Business Ethics*, *148*(1), 169–182. https://doi.org/10.1007/s10551-016-3014-0

Simpson, A., & Quigley, C. F. (2016). Member checking process with adolescent students: Not just reading a transcript. *Qualitative Report*, *21*(2), 377.

Sindhuja, P. N. (2014). Impact of information security initiatives on supply chain performance. *Information Management & Computer Security*, *22*(5), 450–473. https://doi.org/10.1108/IMCS-05-2013-0035

Sindiren, E., & Ciylan, B. (2019). Application model for privileged account access control system in enterprise networks. *Computers & Security*. https://doi.org/10.1016/j.cose.2019.01.008

Singhal, N., & Bhola, P. (2017). Ethical practices in community-based research in nonsuicidal self-injury: A systematic review. *Asian Journal of Psychiatry*, *30*, 127-134. https://doi.org/10.1016/j.ajp.2017.08.015

Sipes, J. B. A., Roberts, L. D., & Mullan, B. (2019). Voice-only skype for sue in researching sensitive topics: A research note. *Qualitative Research in Psychology,* 1-17. https://doi.org/10.1080/14780887.2019.1577518

Sodomka, P., & Klcova, H. (2016). Classification of ERP system services. *Journal of Systems Integration (1804-2724)*, *7*(3), 66–78. https://doi.org/10.20470/jsi.v7i3.263

Soliman, M., Saurin, T. A., & Anzanello, M. J. (2018). The impacts of lean production on the complexity of socio-technical systems. *International Journal of Production Economics*, *197*, 342–357. https://doi.org/10.1016/j.ijpe.2018.01.024

Sprague, C., Scanlon, M. L., & Pantalone, D. W. (2017). Qualitative research methods to advance research on health inequities among previously incarcerated women living with HIV in Alabama. *Health Education & Behavior, 44*(5), 716–727. https://doi.org/10.1177/1090198117726573

Stănculescu, M., Deleanu, S., Andrei, P. C., Andrei, H., & Kotenko, I. (2021). A case study of an industrial power plant under cyberattack: Simulation and analysis. *Energies (19961073*), 14(9), 2568. https://doi.org/10.3390/en14092568

Stefano, A. L. (2017). Quality Systems. A thermodynamics-related interpretive model. *Entropy*, *8*, 418. https://doi.org/10.3390/e19080418

Stiawan, D., Idris, M. Y., Abdullah, A. H., Aljaber, F., & Budiarto, R. (2017). Cyberattack penetration test and vulnerability analysis. *International Journal of Online Engineering*, *13*(1), 125-132. https://doi.org/10.3991/ijoe.v13i01.6407

Stillwell, P., Hayden, J. A., Rosiers, P. D., Harman, K., French, S. D., & Curran, J. A.

(2018). A qualitative study of doctors of chiropractic in a nova scotian practice-based research network: Barriers and facilitators to the screening and management of psychosocial factors for patients with low back pain. *Journal of Manipulative and Physiological Therapeutics*, *4*, 25-33. https://doi.org/10.1016/j.jmpt.2017.07.014

Sun, H., & Jafar, S. A. (2018). Multiround private information retrieval: Capacity and storage overhead. *IEEE Transactions On Information Theory*, *64*(8), 5743–5754. https://doi.org/10.1109/TIT.2018.2789426

Sutton, J., & Austin, Z. (2015). Qualitative Research: Data collection, analysis and management. *Canadian Journal of Hospital Pharmacy*, *68*(3), 226-231.

Syrjä, P., Puumalainen, K., Sjögrén, H., Soininen, J., & Durst, S. (2019). Entrepreneurial orientation in firms with a social mission - a mixed-methods approach. *Cogent Business & Management*, 6(1). https://doi.org/10.1080/23311975.2019.1602016

Tariq, M. I., Ahmed, S., Memon, N. A., Tayyaba, S., Ashraf, M. W., Nazir, M., Hussain, A., Balas, V. E., & Balas, M. M. (2020). Prioritization of information security controls through fuzzy AHP for cloud computing networks and wireless sensor networks. *Sensors (Basel, Switzerland)*, *20*(5). https://doi.org /10.3390/s20051310

Tas, I. D., Yetkiner, A., & Ince, M. (2017). The analysis of articles related to curriculum and instruction field in educational researcher journal (2005-2016). *European Scientific Journal*, *13*(16). https://doi.org/10.19044/esj.2017.v13n16p305

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

Thomas, J., & Galligher, G. (2018). Improving backup system evaluations in information security risk assessments to combat ransomware. *Computer and Information Science*, *11(1),* 14-25. https://doi.org/10.5539/cis.v11n1p14

Tidrea, A., Korodi, A., & Silea, I. (2019). Cryptographic considerations for automation and SCADA systems using trusted platform modules. *Sensors (Basel, Switzerland)*, *19*(19). https://doi.org/10.3390/s19194191

Torten, R., Reaiche, C., & Boyle, S. (2018). The impact of security awareness on information technology professionals' behavior. *Computers & Security*, *79*, 68–79. https://doi.org/10.1016/j.cose.2018.08.007

Trang, S., & Nastjuk, I. (2021). Examining the role of stress and information security policy design in information security compliance behaviour: An experimental study of in-task behaviour. *Computers & Security*, *104*. https://doi.org/10.1016/j.cose.2021.102222

Trnka, S. (2017). The fifty-minute ethnography: Teaching theory through fieldwork. *Journal of Effective Teaching, 17*(1), 28–34.

Turel, O., Liu, P., & Bart, C. (2017). Board-Level information technology governance effects on organizational performance: The roles of strategic alignment and authoritarian governance style. *Information Systems Management*, *34*(2), 117–136. https://doi.org/10.1080/10580530.2017.1288523

Upadhyay, D., & Sampalli, S. (2020). SCADA (Supervisory Control and Data

Acquisition) systems: Vulnerability assessment and security recommendations. Computers & Security, 89, 149-159. https://doi.org/10.1016/j.cose.2019.101666

U.S. Department of Homeland Security. (2016). Critical infrastructure sectors. https://www.dhs.gov/critical-infrastructure-sectors

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. https://doi.org/10.1002/sres.2589

van Manen, M. (2017). Phenomenology in its original sense. *Qualitative Health Research, 27*(6), 810–825. https://doi.org/10.1177/1049732317699381

van Rijnsoever, F. J. (2017). (I Can't Get No) Saturation: A simulation and guidelines for sample sizes in qualitative research. *PLoS ONE*, (7), e0181689. https://doi.org/10.1371/journal.pone.0181689

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. https://doi.org/10.1111/medu.13124

Wang, D., Li, W., & Wang, P. (2018). Measuring two-factor authentication schemes for real-time data access in industrial wireless sensor networks. *IEEE Transactions on Industrial Informatics, Industrial Informatics, IEEE Transactions on, IEEE Trans. Ind. Inf*, (9), 4081. https://doi.org/10.1109/TII.2018.2834351

Wang, H., Lau, N., & Gerdes, R. M. (2018). Examining cybersecurity of cyberphysical systems for critical infrastructures through work domain analysis. *Human Factors*, *60*(5), 699–718. https://doi.org/10.1177/0018720818769250

Wang, S., Pei, R., & Zhang, Y. (2019). EIDM: A ethereum-based cloud user identity management protocol. *IEEE Access*, 7, 115281–115291. https://doi.org/10.1109/access.2019.2933989

Wang, X., & Xu, J. (2021). Deterrence and leadership factors: Which are important for information security policy compliance in the hotel industry. *Tourism Management*, *84*. https://doi.org /10.1016/j.tourman.2021.104282

Weis, D., & Willems, H. (2017). Aggregation, validation, and generalization of qualitative data-Methodological and practical research strategies illustrated by the research process of an empirically based typology. *Integrative Psychological & Behavioral Science*, *51*(2), 223-243. https://doi.org/10.1007/s12124-016-9372-4

Weisburd, D. (2015). The law of crime concentration and the criminology of place. *Criminology*, *53*(2), 133-157. https://doi.org/10.1111/1745-9125.12070

Welsh, B. C., Zimmerman, G. M., & Zane, S. N. (2018). The centrality of theory in modern day crime prevention: Developments, challenges, and opportunities. *Justice Quarterly*, *35*(1), 139-161. https://doi.org/10.1080/07418825.2017.1300312

Wiafe, I., Koranteng, F. N., Wiafe, A., Obeng, E. N., & Yaokumah, W. (2020). The role of norms in information security policy compliance. *Information & Computer Security*, *28*(5), 743–761. https://doi.org/10.1108/ICS-08-2019-0095

Williams, J. K., & Anderson, C. M. (2018). Omics research ethics considerations.

Nursing Outlook, 66(4), 386–393. https://doi.org/10.1016/j.outlook.2018.05.003

Wu, Y., Wang, N., Kropczynski, J., & Carroll, J. M. (2017). The appropriation of GitHub for curation. *PeerJ Computer Science*. https://doi.org/10.7717/peerj-cs.134

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

Xu, M., & Han, W. (2019). An explainable password strength meter addon via textual pattern recognition. *Security & Communication Networks*, 1–10. https://doi.org /10.1155/2019/5184643

Yadav, G., & Paul, K. (2021). Architecture and security of SCADA systems: A review. *International Journal of Critical Infrastructure Protection*, *34*. https://doi.org /10.1016/j.ijcip.2021.100433

Yamin, M. M., Katt, B., & Gkioulos, V. (2020). Cyber ranges and security testbeds: Scenarios, functions, tools and architecture. *Computers & Security*, *88*. https://doi.org/10.1016/j.cose.2019.101636

Yates, J., & Leggett, T. (2016). Qualitative research: An introduction. *Radiologic Technology*, *88*(2), 225-231.

Yilmaz, E. N., & Gonen, S. (2018). Attack detection/prevention system against cyber attack in industrial control systems. *Computers & Security*, *77*, 94–105. https://doi.org/10.1016/j.cose.2018.04.004

Yin, R. K. (2018). *Case study research and applications: Design and methods* (6th ed). Thousand Oaks, CA.

Yin, X. C., Liu, Z. G., Nkenyereye, L., & Ndibanje, B. (2019). Toward an applied cyber security solution in IoT-based smart grids: An intrusion detection system approach. *Sensors (14248220)*, *19*(22), 4952. https://doi.org/10.3390/s19224952

Yu, X., Wang, Z., Li, Y., Li, L., Zhu, W. T., & Song, L. (2017). EvoPass: Evolvable graphical password against shoulder-surfing attacks. *Computers & Security*, 70, 179–198. https://doi.org/10.1016/j.cose.2017.05.006

Zheng, T., Hong, Q., Xi, L., Yizheng, S., & Jie, D. (2020). A security defense model for SCADA system based on game theory. *2020 12th International Conference on Measuring Technology and Mechatronics Automation (ICMTMA),* 253–258. https://doi.org /10.1109/ICMTMA50254.2020.00064

Zhong, C., Lin, T., Liu, P., Yen, J., & Chen, K. (2018). A cyber security data triage operation retrieval system. *Computers & Security*, 76, 12–31. https://doi.org/10.1016/j.cose.2018.02.011

Zhou, L., Chen, J., Zhang, Y., Su, C., & Anthony James, M. (2019). Security analysis and new models on the intelligent symmetric key encryption. *Computers & Security*, *80*, 14–24. https://doi.org/10.1016/j.cose.2018.07.018

Zhou, X., Xu, Z., Wang, L., Chen, K., Chen, C., & Zhang, W. (2018a). APT attack analysis in SCADA systems. *MATEC Web of Conferences*, 01010. https://doi.org/10.1051/matecconf/201817301010

Zhou, X., Xu, Z., Wang, L., Chen, K., Chen, C., & Zhang, W. (2018b). Construction and evaluation of defense-in-depth architecture in SCADA system. *MATEC Web of Conferences*, 01012. https://doi.org/10.1051/matecconf/201817301012

Zoto, E., Kianpour, M., Kowalski, S. J., & Lopez-Rojas, E. A. (2019). A socio-technical systems approach to design and support systems thinking in cybersecurity and risk management education. *Complex Systems Informatics and Modeling Quarterly*, *18*, 65–75. https://doi.org/10.7250/csimq.2019-18.04

Zuopeng, J. Z., Wu, H., Wenzhuo, L., & M'Hammed, A. (2021). Cybersecurity awareness training programs: a cost-benefit analysis framework. *Industrial Management & Data Systems*, *121*(3), 613–636. https://doi.org/10.1108/IMDS-08-2020-0462

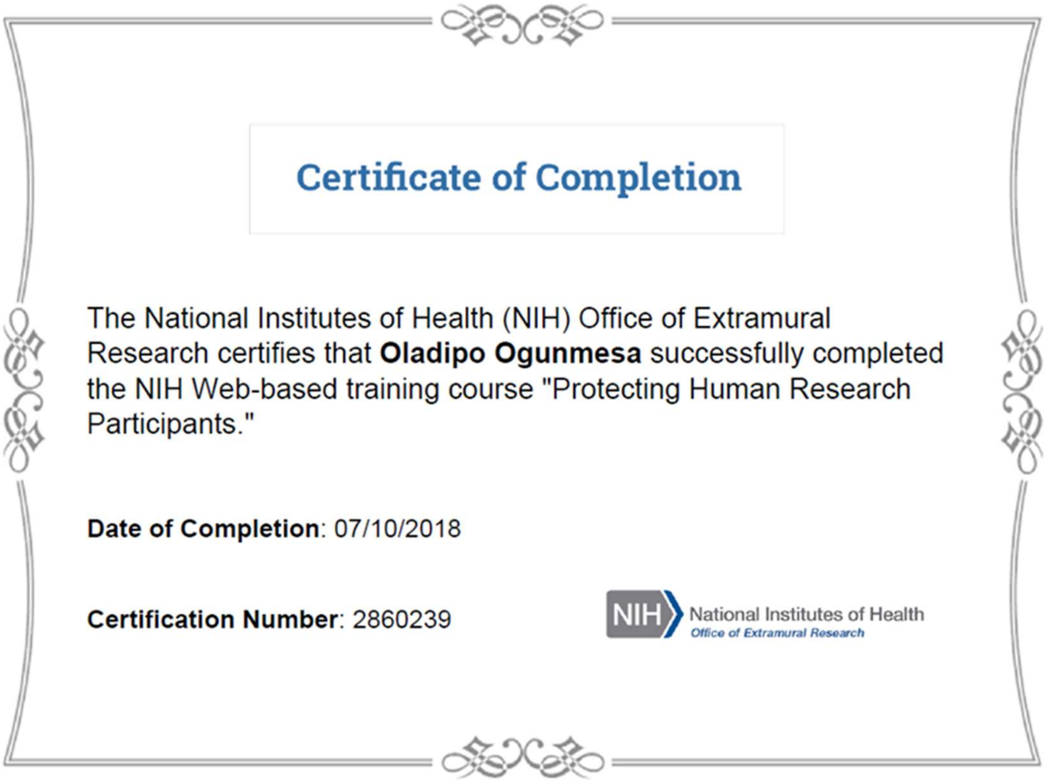
Appendix A: Interview Protocol

Introduction	1. Introduce myself as a doctoral student of Walden University and thank the participants. 2. Brief introduction of the research question: I will be conducting this interview for my Qualitative Research Study based on the Strategies Security Managers Used to Prevent Security Breaches in SCADA Systems' Networks 3. Informed consent confirmation: The main purpose of the consent form is to let you know that participation in this interview is voluntary, and you can choose to stop the interview at any time. The interview will be conducted to ensure there is no harm to both the participant and the researcher. 4. Interview procedure: Inform the participants that the interview will be audio-recorded, and notes will be taken. I will also let the participants know that no identifying information such as name, address, and the organization name will be used. I will tell them that all interview material will be encrypted and stored in a locked container accessible only by the researcher.

	5. Proceed with the interview once the participant indicates readiness to begin and start audio recording.
Initial Probe Questions	1. What is your current role in your organization, and how long have you been in this role? 2. What is your experience either, direct or indirect, with the SCADA systems? 3. What would you say is the most interesting part of your job?
Targeted Concept Questions	1. What influenced the development of SCADA systems' security in your organization? 2. Can you tell me about the tools and techniques used in securing the SCADA systems? 3. How useful are these tools and techniques? 4. How effective and efficient are the methods used in preventing data breaches on SCADA systems' networks? 5. What methods are ineffective in preventing data breaches on SCADA systems' networks? 6. What challenges were faced in executing and implementing these methods?

	7. In your experience, which of these methods, technical, formal, or informal, have you found to be most effective? 8. What impact do technical, formal, and informal strategies have on one another from your experience? 9. In your experience, what are the determining factors on how to implement SCADA security, compliance practices, and cybersecurity training? 10. What can be done to prevent internal attacks by insiders on SCADA systems' networks?
Conclusion	Inform the participants that a follow-up interview will be conducted to review my interpretation of their answers and schedule the interview. Stop audio recordings, and thank the participant for participating in the study.

Appendix B: Training Certificate from the National Institute of Health Office of Extramural Research



Certificate of Completion

The National Institutes of Health (NIH) Office of Extramural Research certifies that **Oladipo Ogunmesa** successfully completed the NIH Web-based training course "Protecting Human Research Participants."

Date of Completion: 07/10/2018

Certification Number: 2860239

NIH National Institutes of Health
Office of Extramural Research