3-6-2024

Cybersecurity Strategies Information Technology Leaders Use to Protect Healthcare Information Systems From Ransomware

Alejandro Ruiz-Caino
Walden University

Walden University

College of Management and Human Potential

This is to certify that the doctoral study by

Alejandro Ruiz-Caino

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

Review Committee
Dr. Donald Carpenter, Committee Chairperson, Information Technology Faculty
Dr. Alan Dawson, Committee Member, Information Technology Faculty

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

Walden University
2024

Abstract

Cybersecurity Strategies Information Technology Leaders Use to Protect Healthcare Information Systems From Ransomware

by

Alejandro Ruiz Caíno

MS, University of Phoenix, 2006

BS, University of Puerto Rico, 2001

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Information Technology

Walden University

February 2024

Abstract

Healthcare organizations' (HCOs') information systems (IS) are prone to increasing ransomware cyberattacks. For HCO information technology (IT) leaders, protecting IS from ransomware attacks is vital because these systems manage large amounts of confidential and sensitive data. Grounded in general systems theory, the purpose of this qualitative pragmatic inquiry study was to explore strategies used by IT leaders in HCOs to protect IS from ransomware attacks. Participants included eight IT leaders from HCOs in the United States responsible for IS protection against ransomware cyberattacks. Data sources included semistructured interviews conducted with the participants via videoconferencing, the researcher's field notes, and 10 online industry documents. Data were analyzed using a thematic analysis; three themes emerged: (a) implement and align technical defense practices with protective technology tools; (b) assess and align security planning elements such as governance, procedures, and policies; and (c) monitor and measure human security elements such as security training and security awareness. IT leaders should implement robust security policies and procedures with proper planning skills aligned with organizational training and awareness plans. The implications for positive social change include the potential to increase security standards that help protect HCOs, thus providing better protection for health IS and personally identifiable patient information.

Cybersecurity Strategies Information Technology Leaders Use to Protect Healthcare Information Systems From Ransomware

by

Alejandro Ruiz Caíno

MS, University of Phoenix, 2006

BS, University of Puerto Rico, 2001

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Information Technology

Walden University

February 2024

Dedication

I dedicate this doctoral study to God as faith has helped me set and achieve my goals. I also want to thank and dedicate this achievement to my father and mother for their love, guidance, and support since welcoming me to the world. To my wonderful wife, Annie, who has filled my heart with inspiration, love, and patience to encourage me in every way possible to continue my goals and our dreams. To my precious son and daughter, Alejandro and Ariana, thank you for understanding and believing that sacrifices and perseverance are critical factors that steer us toward a better quality of life. I feel blessed to have my family close, supporting my academic and personal success.

Acknowledgments

I am infinitely thankful for the unconditional support and encouragement from my family, friends, and academic mentors during this doctoral journey. All of you have impacted me positively during this research study. I thank Dr. Donald Carpenter, who accepted the challenge to become my committee chair. Thank you for the mentorship, enlightenment, wise words, and kind support you projected throughout the study. I also thank the following for their helpful advice and reviews: Dr. Alan Dawson, my second committee member; Dr. Constance Blanson, my university research reviewer; and Dr. Gail Miles, the Doctor of Information Technology program director. This study was made possible because of your dedication to your students and academia. Thank you!

Table of Contents

List of Tables

Section 1: Foundation of the Study

In this study, I sought to identify the strategies information technology (IT) leaders use to protect information systems (IS) from ransomware cyberattacks in healthcare organizations (HCOs). These cyber strategies can help safeguard personally identifiable information (PII) and health information systems (HIS) in an environment and industry where ransomware cyberattacks are on the rise. In Section 1, I provide an overview of the study I conducted.

Background of the Problem

IT leaders in the healthcare industry rely on IT systems as pivotal components to securely manage data communications, operations, and services. As a result of the integration of IS in the healthcare industry, cybersecurity attacks have become an increasing challenge for healthcare IT managers. Ransomware is the most evident cybersecurity risk to U.S. networks, as the attacks encrypt organizational data causing detrimental operational interruptions (Cybersecurity and Infrastructure Security Agency [CISA], 2019). A cybersecurity advisory jointly published by CISA, the Federal Bureau of Investigation, and the U.S. Department of Health and Human Services (2020) noted that the government agencies have reliable information on intensified and looming ransomware threats to U.S. hospitals and healthcare providers and called for industry leaders to take urgent prevention measures against cyberattacks.

As medical technology and IS become more prevalent in the U.S. healthcare system, there is a heightened risk that ransomware may put patient lives and safety at risk by disrupting healthcare providers' access to information they need to provide critical

care (Branch et al., 2019). Ransomware attacks are gaining sophistication and effectiveness, accounting for over 70% of successful cyberattacks on HCOs in 2019 and 2020 (Middaugh, 2021). The increase in ransomware infection cases in the U.S. healthcare industry suggests deficient cybersecurity strategies in IS protection. IT managers from the healthcare industry may benefit from knowledge of strategies to help protect IS from ransomware cyberattacks.

Information Technology Problem Focus and Project Purpose

Ransomware cyberattacks, as well as the number of ransomware variants used to extort organizations, have been increasing during the past five years (Per Hull et al., 2019). In 2020, 560 HCOs in the United States were impacted by 80 incidents of ransomware cyberattacks (U.S. Department of Health & Human Services, Office of Information Security, 2021). The general IT problem was that many HCOs fail to protect IS from ransomware cyberattacks. The specific IT problem was that some IT managers lack cybersecurity strategies to protect IS systems in HCOs in the United States from ransomware cyberattacks.

The purpose of this qualitative pragmatic inquiry study was to explore the cybersecurity strategies some IT managers use to protect IS in HCOs from ransomware cyberattacks. The population for the study included IT leaders working in hospitals in the United States who had implemented cybersecurity strategies to protect IS from ransomware cyberattacks. The research implications for positive social change may include the potential to increase security standards that help protect HCOs' IS, thus providing better protection for HIS and PII.

After considering both quantitative and mixed methods, I used the qualitative method for this study because I intended to thoroughly examine a social phenomenon. When using qualitative research, the environment in which the research takes place can affect the study's findings, as it examines a social phenomenon in detail, uncovering experiences and perceptions (Ezer & Aksüt, 2021). Quantitative studies involve statistical analyses that develop based on hypothesis testing (Reich, 2021). The quantitative method did not suit this research because neither a mathematical model nor hypothesis testing were involved. A mixed-methods approach without quantitative or statistical data to test a hypothesis by associating variables is unfavorable, as incorporating only qualitative or narrative data may not provide sufficient evidence to effectively examine the connections between different factors in the research (Ranieri et al., 2019). A mixed-methods approach would not fit this study because I neither collected nor interpreted quantitative data findings.

I chose to conduct a pragmatic qualitative inquiry after also considering phenomenology and ethnographic research designs. My rationale was that I intended to use descriptive language in analyzing and presenting the results. Pragmatic inquiry emphasizes the constantly changing and evolving nature of research phenomena; its interdisciplinary nature is appealing in a context where researchers are increasingly adopting theoretical and methodological frameworks across disciplinary research boundaries (Siitonen et al., 2021). Researchers utilize a phenomenological design to understand cognition and expectations to capture the reality of a phenomenon (H. Williams, 2021). For this reason, a phenomenological design was inappropriate for this

study. Researchers use ethnography to gather firsthand accounts and insights from community members about their experiences and perspectives related to these events (Danley, 2021) I opted against using an ethnographic design because I was not looking to document the cultural experience of IT leaders.

The conceptual framework for this study was the general systems theory (GST). The Austrian scientist Karl Ludwig von Bertalanffy first published GST in 1968 (Van Assche et al., 2019a). Although GST theory has been around for decades, researchers are reviving efforts to apply it to IS investigations (Chatterjee et al., 2021). GST introduced universal principles that dominate every system, presenting them as interrelated components of a larger whole that are alike with structure and function similarities but acting independently of their particular domains (von Bertalanffy, 1968). From a GST perspective, systems are composed of and exist within a hierarchy of systems (O. Johnson, 2019). GST attunes to a holistic approach to healthcare-related issues and problems (Katrakazas et al., 2020); therefore, it was suitable for my study. Healthcare can be seen as a mega-system consisting of subsystems (Katrakazas et al., 2020). A GST approach can be used to address challenges faced on a microlevel such as a hospital system as was at the macrolevel of a country or global system (Katrakazas et al., 2020). Cybersecurity issues need a holistic view (Melon & Hernandez, 2020) to approach problem solutions.

Research Question

What cybersecurity strategies are used by IT leaders to protect HCOs IS from ransomware attacks in the United States the United States?

Assumptions and Limitations

Assumptions

Assumptions consist of unsubstantiated claims or facts used by researchers to support the research (Caster, 2020). I have identified three assumptions in this study. The first assumption was that the participants provided candid responses to the interview questions. Participant anonymity is discussed with the participant before conducting the interviews to promote honesty. A second assumption was that the data collection process provided sufficient data to answer the central research question. A final assumption was that the research sample represents the studied population allowing for the transfer of study findings to other HCO IT leaders.

Limitations

Research limitations can be defined as uncontrollable boundaries and constraints that directly influence the study results (Caster, 2020). This study was limited to IT leaders from HCOs in the United States. I gathered data by interviewing the participants. The study's sample size and the participating IT leaders' varying levels of experience levels are limitations of the study.

Significance of the Study

Contribution to Information Technology Practice

Cybersecurity is an essential part of security in today's technological reality. Lately, there has been an increase in ransomware cyberattacks that have disrupted HCOs operations. In this study, I explored the strategies that IT leaders use to protect IS from ransomware cyberattacks contributing to improving IS security in HCOs. By

interviewing IT leaders and analyzing relevant industry documents, I sought to gain insight on ransomware protection practices, including technical or nontechnical control strategies. Data analysis may reveal practical actions for IT leaders from the healthcare industry to protect U.S. HISs from ransomware cyberattacks.

Implications for Social Change

This research provides valuable insights into current practices for fighting ransomware. The study findings may help other researchers to develop strategies and techniques to protect HCOs from ransomware, while also helping secure HIS and PII from being attacked. Furthermore, the study has the potential to foster positive social change because it could help other IT leaders build knowledge to increase cybersecurity awareness and expertise in ransomware cyberattacks. As cyberattacks increase, more IT leaders with information security knowledge will be needed in across industries, including healthcare. As more IT managers integrate into organizational structures to manage future cybersecurity threats, an opportunity for employment demand may reduce the unemployment rate while improving the quality of life of U.S. employees and patients.

A Review of the Professional and Academic Literature

In this pragmatic qualitative inquiry study, I explored strategies that HCO IT leaders use to prevent and protect healthcare IS from ransomware cyberattacks. This literature review includes discussion of professional and academic literature that addresses such strategies. In reviewing the literature, I sought to draw out the connection of research to the study's conceptual framework. The success of a literature review

depends on the ability to summarize and integrate existing knowledge about a specific subject (Kraus et al., 2020). This critical part of the research involves analysis of academic resources on the selected subject. A literature review helps the researcher synthesize findings to present evidence on a meta-level and continue investigating areas where research is lacking, which is an essential component of theoretical frameworks and conceptual models (Snyder, 2019). A good literature review helps guide researchers toward improved efficiency and productivity while documenting future research progress in a novel study area (Kraus et al., 2021).

To develop this literature review, I used various online resources. Ninety-four references comprise the content of this synthesis and analysis. Eighty-two of the 94 references were published within the last 5 years, for 87.2% of the total references. Eighty of the 94 references were peer reviewed, forming 85.1% of the total references. This document includes 243 sources in total.

To narrow the literature search, I used the following keywords: *information systems security*, *healthcare information systems* (HIS), *healthcare organizations*, *ransomware*, *cyberattack*, *personally identifiable information* (PII), *healthcare organizations*, *hospital*, *phishing*, and *information system vulnerabilities*. I verified peer-reviewed articles using digital object identifiers, International Standard Serial Numbers, and Ulrich's Global Series Directory. Works without a digital object identifier or International Standard Serial Number were verified with Ulrich's Global Series Directory. I gathered scholarly and academic resources electronically by searching on Google Scholar, Elsevier, ProQuest, and IEEE Xplore Digital Libraries.

The literature review addresses significant concepts of ransomware, such as their functioning during cyberattacks, development, system effects, outcomes, and consequences. Next, the literature review will be aligned with the GST conceptual framework. The narrative will consist of principal notions, GST application to healthcare and cybersecurity settings, a discussion of studies that featured GST as the conceptual framework, and other frameworks supporting and opposing GST. Finally, I will examine the strategies used by IT leaders in HCOs to protect IS from ransomware cyberattacks.

Conceptual Model

General Systems Theory

I chose the GST as the conceptual framework for this study. GST is also known as the theory of open systems (Van Assche et al., 2019b). von Bertalanffy (1968) stated that a system is a compilation of interacting units that construct a united whole. A system is comprised of intermingling components and has a particular purpose to fulfill; so, the individual components lose autonomy corresponding to the system's intention (Panetto et al., 2019). A system comprises interrelated and interdependent components (von Bertalanffy, 1968), forming a functional entity. Systems outline space and temporal boundaries that surround and influence their relationship with the environment while described by their structure and purpose (CUI Weicheng, 2021). Systems arise as independent operation links that intertwine between distinction of internal operations and external events (Van Assche et al., 2019a). A systematists perception identifies the world as a world of systems where things interact between their internal dynamics and environment, following a level structure of elements that work together to generate

subsystems (Weber, 2020). In general, GST centers on the existing relations among system components.

According to Owen Johnson (2019), GST was developed as a framework to unite interdisciplinary science, following the works of the Austrian Karl Ludwig von Bertalanffy during the post-WWII era. von Bertalanffy's GST concepts were constructed prior to and during WWII but were published when postwar systems concepts and approaches were catching up with scientists (O. Johnson, 2019). von Bertalanffy and Sutherland (1974) emphasized the need of interaction with the external environment, distinct from the classical school theorists like Max Weber, Frederic Tailor, and Henry Fayol, who introduced the concept of closed systems to organizations (Chikere & Nuwoka, 2015). There was a sudden surge in open systems movement, helping develop the principles and theories regarding computerized systems (O. Johnson, 2019).

System science, philosophy, and technology are considered systems theory application areas (von Bertalanffy, 1968). Jung and Vakharia (2019) presented systems theory as a flexible and multidisciplinary theory used in different areas of organizational studies. Systems theory is an interdisciplinary scientific field that studies complex phenomena involving systems and their relationships (Mele et al., 2010). von Bertalanffy wanted to develop a more general approach to systems, and from the open systems approaches, the researchers developed engineering, ITs, and cybernetics (Jung & Vakharia, 2019). von Bertalanffy's open systems view allowed interaction with the environment, emulating biological functions looking for resilience (Van Assche et al., 2019b). The final state of closed systems is defined by its initial conditions. The final

state of a closed system is represented by initial conditions, contrary to open systems, where the final state is steady because it can be attained from diverse initial conditions to present equifinality (von Bertalanffy, 1951).

Since the 16th century, scientists have explained singularities by examining the essential components of a system autonomously from one another. Still, during the 20th century, testing of singularities with various field lenses evolved on wholeness and how individual parts fit the puzzle wholly (Šijan et al., 2019). The shift in focus from studying individual units towards the completeness of complexity of the interrelated components aided in the development of an open framework under all sciences (O. Johnson, 2019).

Before von Bertalanffy developed GST, other researchers had published similar concepts. Poustilnik (2021) noted Aleksandr Bogdanov's idea of tektological assembling like a universal tool to build any organization was developed between 1912 and 1917. Tektology was viewed by researchers as a universal organizational science from 1913 to 1922, presenting knowledge in the organization systems model (Poustilnik, 2021). Aleksandr Bogdanov was seeking to reformulate the general laws of organization with holistic, evolving experiences and systemic development circumstances (Yan et al., 2020). By uniting holism and systems theory, Bogdanov developed the transdisciplinary science of physical organization (Yan et al., 2020).

In 1937, during a philosophy seminar at the University of Chicago, von Bertalanffy first presented his GST concepts after researching systemic singularities without their scientific nature mattering (Šijan et al., 2019). He created his systems approach from a biological viewpoint as he developed the organism system theory before

the 1950s (Lavassani & Movahedi, 2021). He aligned research on the design and what its environment responds to continuously (Van Assche et al., 2019b). After the 1950s, von Bertalanffy focused on the methodology development of science, leading to GST in the 1960s (Lavassani & Movahedi, 2021). According to Šijan et al. (2019), von Bertalanffy won the First World Cup scientific award in 1956, founding the Scientific Institute Society for General Systems Research. GST's development in 1968 concentrated on determining the general theory as a whole with its interconnectedness of components and system legalities (Van Assche et al., 2019b). GST's mission includes detecting and defining systemic legalities from complex phenomena in systems to solve problems (Šijan et al., 2019).

von Bertalanffy followed the notion that systems are composed of a set of similar characteristics and properties no matter the discipline. He emphasized the relationship principles of structure and operations of any system, no matter its dimension. GST was viewed as an interdisciplinary theory with a universal pertinency and shared etymology (von Bertalanffy, 1968). von Bertalanffy wanted to unite different sciences conducive to general principles which all systems could use. GST involves the principles of dynamic adaptive and self-organized equilibria (Tretter, 2019). von Bertalanffy's GST proposed the existence of models and guides that make systems of different types, processes, and relations in system environments come to life as a whole. GST looks at systems as elements of a bigger whole, representing resemblances in structures and functions but having autonomy from their domains while merging organizational hierarchies, multivariable interaction, and goal-oriented processes (von Bertalanffy, 1968) to achieve

optimization. GST dynamic capabilities present the system's capacity to react to changing environments by restructuring static and inflexible ordinary capabilities (Schriber & Löwstedt, 2020).

Prior Studies Featuring General Systems Theory in Healthcare and Cybersecurity Settings

An HCO is considered an open system because "it is defined by energy transformation, dynamic steady state, negative entropy, event cycles, negative feedback, differentiation, integration and coordination, and equifinality" (Meyer & O'Brien-Pallas, 2010, p.2828). Healthcare is a mega-system consisting of different subsystems that can help address challenges and opportunities at every level, including at the micro level (hospital system) and macro level, such as a world system (Katrakazas et al., 2020). Recent healthcare research has involved the practical implementation of GST. Katrakazas et al. (2020) present a GST data framework utilized to detect equilibria levels and gain stabilization with the opportunity to predict capability over time in the hearing loss screening area, therefore increasing treatment and management strategies on public hearing health methods. Redox, a GST-inspired conceptual framework, was presented by Santolini et al. (2019) as they searched to explain a patient's metabolic pathways and cellular bioenergetics from a multi-level holistic systems biology approach. Another GST framework was developed by Folami et al. (2019), which focused on studying the nursing process and its affecting factors, as it aimed to obtain overall positive attitudes from nurses. In another study, Gonul Kochan et al. (2018) used GST for hospital research aiming to study how information sharing impacts a hospital supply chain. The research

presented positive results on the utilization of cloud-based information sharing because of the opportunity to have real-time inventory while decreasing inventory variability, translating into better customer service.

There exists a practical implementation of GST in the information security and cybersecurity environment. Melon and Hernandez (2020) mention that IT leaders should view and understand cybersecurity issues from a holistic point of view. Tarafdar and Bose (2019) focused on a systems thinking-based approach to resolve cybersecurity complications when examining India's digital identity program with Systems Theoretic Process Analysis. Tarafdar and Bose (2019) study helped identify system security vulnerabilities while also identifying security controls that decreased threats. Bier and Gutfraind's (2019) research defined and proposed a new security index denominated defensibility that focused on comparing the asset value distributions in the system's threat nature. Hu et al. (2021) research used system theory to view security, education, training, and awareness (SETA) programs as organizational systems that test employees' effects towards the intentions to adhere to security policies. Results presented that the SETA program has more effect when encouraging extra-role behavioral intention than compliance intentions.

According to Adkoli and Parija (2019), there exist three major components in every system: inputs, processes, and output. By studying inputs transform into outputs, researchers view problem-solving systematically to identify specific patterns and relationships. Organizations share similarities and patterns in their inputs, processes, and outputs to accomplish organizational goals. I consider an organization a system because it

has combined parts that aim through organized attempts to be more effective and efficient (Chikere & Nuwoka, 2015); consequently, HCOs are also systems. Post et al. (2020) mention that a system's three components are its elements, interrelationships, and boundary. These components are necessary to reach the system goal. Coordination exists among all subcomponent parts to guide all organizational components to share the final destination. Constructs or processes remain the same during the system's life. At the same time, interrelationships between elements show the system's state without changing, allowing one to identify if the state of a system was employed, as the boundary determines who and what enters and exits the system (Post et al., 2020).

The nursing area is an example of a system element of an HCO. Nursing is possible as synchronization of different systems interact, because without HIS, nurses could not work competently or comply to standards (Ayala et al., 2019). The same situation applies to medical staff relying primarily on HIS to complete their medical tasks. The relationship between these HCO system elements follows technical and non-technical cybersecurity controls, regulating the cybersecurity inputs and outputs of the system. Secure IT settings help organizations and stakeholders land the best path for patient care and well-being (O. Johnson, 2019). Strong cybersecurity allows patients to obtain better healthcare services (Tully et al., 2020), ensuring business continuity for normal operations.

Chikere and Nuwoka's (2015) study proposes organizations adopt the systems approach to increase growth and profitability as systems support other systems and balance the whole organization preventing failure. Because IS coordinate and support

stakeholder organizational activities, it is deemed an essential component of an HCO system as it helps maintain organizational operations by providing healthcare to the population (O. Johnson, 2019). Because HIS is responsible for the data exchange between the system components, HIS data must be safeguarded and secure focusing on the Central Intelligence Agency triad of cybersecurity factors: confidentiality, integrity, and availability. A systems approach can attract healthcare IT leaders because systems viewpoints and standards are appreciated and often used in medicine, biomedical sciences, therapy approaches, informatics systems, and HCOs (O. Johnson, 2019). HCO IT leaders share responsibility for patient health information (PHI) handling as they balance medicine and IT to provide healthcare service improvements in processes, care pathways, and health delivery systems. Securing HIS from ransomware is necessary to maintain uninterrupted communications, processes, and operations transforming effective patient care in HCOs. Applied healthcare obstacles can use GST as a solution tool (O. Johnson, 2019).

Holism is considered a fundamental principle in the context of GST as it posits that the characteristics of a system, encompassing biological, chemical, physical, social, economic, mental, psychological, and other aspects, cannot be fully elucidated by merely aggregating its individual components (Tadros, 2020). The whole system defines and determines the part's roles as "the whole is more than a sum of its parts" (von Bertalanffy, 1968, p. 18), borrowing the holistic system principle from Aristotle and the Gestalt movement (Turner & Baker, 2019). The parts structure and interaction between each component determine system properties, where system behavior is independent of

the components' properties (Chikere & Nuwoka, 2015). A holistic approach views the system working in coherence as a functional unit. GST approaches systems problems within stated boundaries (Turner & Baker, 2019), as the system works harmoniously as an entity when interconnected to its components. Applying a holistic approach to an HCO cybersecurity problem may lead to the discovery of practical strategies that protect HIS from ransomware cyberattacks. According to Weber (2020), GST could be used to show how the various human and non-human components in the phenomena interact systemically toward a common purpose. Because GST focuses on purposiveness (Chatterjee et al., 2021), it may help view and identify the relationships between healthcare IS subcomponents, including technical and human interrelated subsystems working together with the IS to achieve a common goal within the changing environment. Successful strategies from three perspectives, including users, technology, and IT capability, align through GST from a cybersecurity perspective (Khayer et al., 2020).

In GST, internal complexity links to external complexity and external resources, so attention is given to the internal and external environments to understand a complex system evolution (Van Assche et al., 2019b). Lazlo and Krippner (1998) present a four-step approach analysis that can produce a possible common rubric of systems theory that includes an embedding context, followed by defining the components of the system whole within the framework. The third step involves identifying the specialized subcomponents, emphasizing on deciphering the structures, compositions, and operation modes, while the final step embeds context by integrating the perspective from previous actions to create a general understanding of the phenomenon upon external and internal

contexts (Lazlo & Krippner, 1998). The function and structure of relationships between components and subcomponents can present an understanding of the entity or process from the system's components roles and tasks for the whole complete system. (Lazlo & Krippner, 1998).

Theories Supporting General Systems Theory

GST creation was inspired by biology, thermodynamics, systems engineering, and early computer science (Van Assche et al., 2019a). GST considered the unconscious and conscious utilization of models of non-biological terms, including machines and computers, while searching to explain in biological terms (von Bertalanffy, 1968). GST benefited from the parallel emergence of cybernetics and information theory (Lazlo & Krippner, 1998). GST covered academic fields like biology, math, psychology, sociology, and philosophy (von Bertalanffy, 1968).

Organismic systems medicine is intended to connect these knowledge fields from the treatment of diseases' medical points of view (Tretter et al., 2021). von Bertalanffy developed this approach to medicine in the 1930s by von Bertalanffy based on perspectives of developmental biology, holistic psychology (Van Assche et al., 2019a), and a theory-oriented approach (Tretter, 2019). In the 1920s, von Bertalanffy commenced working on the integration concept, as he empirically studied the processes of self-organization in organisms, leading to the evolution and development of organismic systems medicine (Tretter, 2019). Although ransomware can be seen as an IS disease from a biological point of view, I'm not focused on giving a medical point of view to cybersecurity elements that GST does attend to.

GST has also been valuable for theories of resilience thinking and social-ecological systems, as they are the leading forms of sustainability thinking (Van Assche et al., 2019b). There have also been attempts to use the general evolution theory in social systems design forming the evolutionary systems design, which is oriented towards identifying different evolution paths that fulfill the idea of sustainable development of life in this planet (Lazlo & Krippner, 1998.). Since I am not studying sustainability issues, I did not select organismic systems medicine, resilience thinking, or general evolution theory as theories for my study.

Another GST-supporting theory is the critical systems theory, which involves constant critical reflection methodology following a solid trend in humanistic systems work (Xin et al., 2022). Critical systems theory was drawn from system theory ideas as Niklas Luhmann and Gunther Teubner intertwined both with Karl Marx's critical theory movement theoretical resources (Möller, 2022). According to Watson and Watson (2011), it was Churchman during the 1970s that initially developed and discussed the foundations of the critical systems approach. While following the science of operations research and management, Churchman (1970) focused on parting ways from a sound operational hard systems approach of the natural sciences refocusing on rationalism and empiricism (Watson & Watson, 2011). Churchman (1970) united Kant's belief in systemic judgment of systemic data and Hegel's belief in additional systemic reviews. Churchman (1970) was looking for an "irrational systems approach," recognizing "there can be no one optimal, absolutely right judgment or solution to system problems" (Watson & Watson, 2011, p. 67).

Watson and Watson (2013) noted that systems thinking researchers applying in human systems wished to evolve towards a more analytical and social attitude inside the systems thinking and practice. These researchers developed critical approaches to systems thinking while centering on Habermas's epistemological and ontological sight (Watson & Watson, 2013). Researchers who use critical systems theory group methods of systems thinking focusing on the fairness and power of those potentially disadvantaged by boosting voice and communicating multiple values and vantage points toward decisions of the problem (Jackson & Sambo, 2020). They assess the problem by distinguishing between the fundamental point of views, assumptions, and biases, but also having of the existing methodologies, strengths, limitations, and adoption implications (Monat et al., 2020). The total systems intervention approach was developed and supported from a critical systems theory viewpoint, as it assumes that problem-solving methods can complement; therefore, each problem situation should be matched by the researcher with the best method for each side of the problem (Lazlo & Krippner, 1998). I did not select the critical systems theory/total systems intervention approach as it mainly focused on humanistic problem-solving methods, which I do not plan to study with this research.

Action theory is considered a GST-supporting theory as it follows a holistic systems approach that studies its environment but limits its scope to social situations, contrary to GST, which is applied in any universal setting (T. Williams et al., 2022). Talcom Parsons developed the action theory to clarify how a distinct social order's micro and macro qualities present structural integrity along with member contribution (Aslan et

al., 2020). Parsons constructed a theoretical framework grounded in an action-oriented perspective and a voluntaristic theory of action inspired by classical sociologists such as Durkheim & Weber (Ormerod, 2020). Action theory explores a process that presents the opportunity to generate new understandings through action (T. Williams et al., 2022). I did not select action theory because Craig (2019) states that action theory leans toward individual behavior by predicting human behavior outcomes and because my research does not intend to investigate social actions or behaviors.

Theories Contrasting With General Systems Theory

The principal investigative improvement of the systems approach involves reducing dynamics compared to reducing components, as experienced in classical science methodologies (Lazlo & Krippner, 1998). Newtonian science rivaled classical science, where determinism, reductionism, and separation are the foundation principles of all existence (Walton, 2021). The reductionist strategy aims to minimize the concepts necessary for minimum scientific statement explanations (Ribatti, 2021). In reductionist determinism science, the researcher gives up understanding reality while adopting quantitative measures to process the numeric data of past and present inferences (Mihai, 2021). As I am not looking to measure inference data, I selected GST for this research. Another reason reductionist determinism was not chosen was that Mihai (2021) states that the path is legitimate where the subject of change has no active role in choice-making.

The evolution idea inherent in GST does not focus on Darwinism perse, as for GST, the survival of the fittest view does not necessarily drive evolution as the

development of complexity always involves testing alternatives, like the complex adaptive system (CAS) theory (Van Assche et al., 2019b). In 1984 Prigogine and Stengers constructed and presented the theory of CAS (Spannring & Hawke, 2022). CAS organization is radical as it involves analyzing a system's processes, structures, and elements to generate the functions, components, and structures (Van Assche et al., 2019b). The two theories are similar as they relate to the more extensive system with related elements. CAS network system is composed of nonlinear subsystem components that depend on each other (Y. Shi et al., 2021). Hodiamont et al. (2019) present CAS under the view that although the individual components of a system are identified and studied by the researcher, it does not suggest complete comprehension of the system's behavior exists. In turn, GST enhances identifying problems, trends, and relationships among components to predict the whole system's behavior as CAS follows a dynamic process challenging the cause-and-effect expectations (Hodiamont et al., 2019*).*

Ransomware

The term *ransomware* was defined by Davies et al. (2021) as a malicious software class that attacks the victim's system or data by disrupting system availability with unauthorized data encryption or system lock until the attacker receives the stipulated ransom. Ransomware has been demonstrated to give rise to intricate attack pathways featuring numerous mutations and variations. This malicious software is capable of encrypting files or restricting access to devices, typically demanding payment in cryptocurrency to restore functionality (Reshmi, 2021). The ransomware employs cryptographic techniques to encrypt the information on the infected computer, rendering

it inaccessible until the specified payment is made, facilitating the decryption process and restoring system access (Ren et al., 2018). Ransomware's primary purpose involves disrupting business operations to create fear and chaos among managers, so the administration considers paying the ransom in hopes that the cyber attackers return the access or choosing not to pay the ransom while restoring operations (Computer Security Research Center [CSRC], 2021).

Ransomware's intentions include attacking and gaining unauthorized control of computer networks, systems, and data following the existing two ransomware classes. The ransomware crypto class follows an encryption attack on the target's files, and the locker class follows a locking attack on the target's device, demanding a ransom for access recovery (Maigida et al., 2019). Different ransomware variants can confuse code, making their identification harder, varying on their polymorphous and metamorphous actions (Reshmi, 2021). Delivery methods of ransomware, such as ransomware-as-a-service (RaaS), embed blockchain technology and the interplanetary file system peer-to-peer network (Karapapas et al., 2020). RaaS permits attackers to affiliate with a RaaS program that can propagate ransomware to prospective victims that would pay the ransomware's software author by interchanging the decryption key while splitting the ransom's profits (Karapapas et al., 2020).

Healthcare cybersecurity is at risk due to a considerable scarcity of information security leaders, the pervasive utilization of obsolete equipment, and software vulnerabilities in related technologies and devices (Tully et al., 2020). Low cybersecurity budgets and the absence of a formal security program or dedicated security leader also

widen the possibility of being vulnerable to attacks (Abraham et al., 2019). These are the main obstacles healthcare IT leaders face regarding HIS and PII cybersecurity protection against ransomware and other malware. Attending each of these obstacles with the correct cybersecurity strategies should be a priority for the industry, organization, and IT leaders.

Ransomware in Healthcare Organizations and Health Information Systems

Information security is becoming increasingly crucial to exist and operate in the modern technological landscape (Kuzminykh et al., 2021). Industries and businesses use IS to organize data into useful decision-making information that supports their operations, goals, and mission. The healthcare industry has been no exception, as healthcare organizations have fully digitalized their sensitive business operations connected to the cloud and internet-based infrastructures (Kiser & Maniam, 2021). Healthcare IT has evolved digitally during this decade, quickly advancing patient service and improving patient care, although embracing the possibility of encountering new cybersecurity vulnerabilities (Richardson et al., 2021). Patient health improves whenever cybersecurity improves (Tully et al., 2020).

The success of a healthcare IS is centered on the capability to collect, process, and share PHI (Ruotsalainen & Blobel, 2020). Ransomware causes HIS operation disruptions, endangering patients' care and lives, while the attackers hold captive the access to confidential PHI. Cybercriminals may be able to shut down and disconnect access to devices, servers, and network infrastructure, disrupting patient records, imaging, surgical services, medical devices, and medical appointment systems (Muthuppalaniappan &

Stevenson, 2021). A rise in ransomware cyberattacks incidence on HCOs expresses the susceptibility of critical patient healthcare services against such cybersecurity threats (Scalco et al., 2021). Ransomware cybercriminals altered tactics to focus on attacking high-value institutions like hospitals (Abdullahi Yari et al., 2021). Cybersecurity investments for HCOs are necessary as cybersecurity breaches can disclose PHI and interrupt clinical emergency or lifesaving care services, potentially resulting in patient deaths (Muthuppalaniappan & Stevenson, 2021). Uninterrupted access to healthcare information helps optimize patient treatments and critical care; however, ransomware cyberattacks could threaten U.S. HCOs, risking patients' lives and safety.

Cybersecurity incidents are an increasing challenge for the healthcare industry (Tully et al., 2020), especially ransomware cyberattacks. Cybercriminals consider HCOs major targets for ransomware attacks due to the PHI's data vitality and confidentiality (Humayun et al., 2021). Healthcare is the most impacted industry by ransomware cyberattacks because cybercriminals value PHI with high profitability cost in the dark web (R. Kumar et al., 2020). When attackers gain access to PHI, they demand a ransom payment in return or use it to perpetrate identity theft to acquire free-of-charge medical procedures or prescriptions or sell them on the black market (Kiser & Maniam, 2021). Any cyberattack can damage the patient's care and well-being while negatively impacting the HCO's brand image (R. Kumar et al., 2020). HCO IT leaders should be prepared as Interpol issued a warning regarding ransomware gangs using malware on HCOs because of the high impact and possibility of high ransoms (Richardson et al., 2021). Despite legislation and the development of technology designed to protect electronic health

records, cyberattacks keep increasing (Kessler et al., 2020). Although the law, regulation, and policy help shape and establish cybersecurity frameworks, Tully et al. (2020) mention that HCOs continue to struggle with information security practices as current incidents have revealed the significance of engaging this cyberthreat using a stronger evidence-based framework to protect HCOs & HIS.

HCOs have increased the adoption of IS in clinical and non-clinical settings (Kuek & Hakkennes, 2020). Effective ICT coordination with secure protection can be complex for an IT leader. HCOs' cybersecurity vulnerabilities are composed of multiple technical and organizational factors, making each cyberattack unique due to the different aims, lengths, and tools involved (Filipec & Plášil, 2021). The most common ways an HCO system can become infected with ransomware include an employee unknowingly downloading malicious software into their electronic device clicking on a link or attachment that was sent in a phishing email; another sources is embedded malware coding located in interactive public health associated situations like pandemic related maps and internet websites (Muthuppalaniappan & Stevenson, 2021). Healthcare needs more security research to help organizational decision-makers understand and enhance IS security and efficiency goals (Omoyiola, 2020).

Laws and Regulations Related to Information Security in Healthcare Organizations

HIS security is closely bounded by the Central Intelligence Agency triad pillars of information security, as they are closely regulated by federal, state, and local laws and policies. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Privacy, Security, and Breach Notification Rules are the primary federal acts that

protect health information by granting rights to patients and limiting how PHI can be used and shared with others (Office of the National Coordinator for Health Information Technology, 2018). The act promoted incentives for digital record adoption. HIPAA establishes national standards to protect the PHI of users only in the United States (Tarikere et al., 2021), as the U.S. government values the digitalization of information in the healthcare industry (Wu & Trigo, 2021). In 2005, the Security Rule establishment focused on digitally stored PHI (Thompson, 2020). It establishes how PHI is kept secure and protected with administrative, technical, and physical safeguards (Office of the National Coordinator for Health Information Technology, 2018). HIPAA authority and enforcement were granted to the U.S. Department of Health and Human Services in 2006 when the Enforcement Rule took effect and started to investigate acceptable privacy violations (Thompson, 2020). HIPAA also addresses cybersecurity by requiring strict reporting for breach incidents of PHI if the incident has exposed more than 500 individuals' data (Tully et al., 2020). HIPAA regulations also require an emergency manager in charge of the organizational emergency preparedness and disaster recovery plans, including the cybersecurity-specific plans for the HCOs (Tully et al., 2020). The Health Information Technology for Economic and Clinical Act (HITECH) of 2009 incentivized HCOs to adopt digital medical records (Thompson, 2020). The Patient Protection and Affordable Care Act of 2010 led to a historical advancement of health equity in the United States that also transformed the digital healthcare industry. If healthcare providers do not meet the requirements, they might incur the possibility of remediation costs, legal fines, brand damage, and business loss (Chung, 2020).

Healthcare rules, laws, and regulations act as an information guide and compliance to diminish IT difficulties, such as: improving healthcare processes to reduce medical errors; e-services development to connect stakeholders, acceptance and continued use of HIS; HIS effective management, HIS security threat reduction on PHI, and financial assessment viability to maintain costs down (Haried et al., 2019).

The average cost of data loss is more significant for an HCO than for organizations from other industries (Bhuyan et al., 2020). Cybersecurity challenges for healthcare include actualizing HCO IT leaders' knowledge to use information security strategies to protect their IS, as noncompliance can lead to legal issues, expensive regulatory fines, and service downtime. Maryland's State legislation SB623 prohibits the interruption of computer services in healthcare facilities (Scalco et al., 2021). The lack of basic IT security measures in healthcare systems is possible (Eichelberg et al., 2020). Penalties and fines imposed by bodies such as the Office of Civil Rights, Health and Human Rights further increase the financial burden on healthcare organizations, even though it incentivizes companies to improve their cybersecurity (Bhuyan et al., 2020) against ransomware. Although the legal and regulatory environment provides a foundation, there is a need for a robust and evidence-based framework to fight and mitigate healthcare cybercrime (Tully et al., 2020)

Strategies to Protect Against Ransomware Attacks

Healthcare IT leaders should adopt a proven ransomware framework that can secure IT and operations to protect HIS from ransomware systemically, as experts recommend a multi-prone approach to avoiding it and dealing with it in case HIS suffers

a cyberattack (Richardson et al., 2021). The NIST cybersecurity framework on ransomware risk management mitigates ransomware through five categories: identify, protect, detect, respond, and recover (Barker et al., 2022). This research focuses on HIS protection while focusing on the NIST ransomware framework as it "develops and implements the appropriate safeguards to ensure delivery of critical services and support the ability to contain the impact of a potential ransomware cybersecurity event." (Barker et al., 2022, p.5). The protection category comprises the following subcategories: identity management, authentication, and access control, awareness and training, data security, information protection processes and procedures, maintenance, and protective technology (Barker et al., 2022).

Identity management, authentication, and access control are considered the first subcategory of the protection category. Physical and logical assets and associated facilities access must be restricted to authorized users, processes, and devices while having constant risk assessments of non-authorized activities and transactions (Barker et al., 2022). Most ransomware cyberattacks occur remotely through network connections (Richardson et al., 2021), often starting with credential compromise (Barker et al., 2022). Proper credential management, including multi-factor authentication and remote access privileges, are part of the protection mitigation recommendations for this subcategory and network segmentation (Barker et al., 2022). Information technology and the operational technology network need independence validation as part of ICS functions and safety instrument systems (Wan et al., 2021).

The second subtopic for protection, awareness and training involves developing SETA programs for system users regarding cybersecurity responsibilities, policies, procedures, and agreements (Barker et al., 2022). Eliminating unsafe practices and having secure configurations help mitigate ransomware cyberattacks. Failures in information security, including technical and administrative controls, can be avoided with SETA program implementation. When stakeholders gain knowledge of information security, it contributes to a solid organizational security culture (Kritzinger et al., 2022). SETA programs are the most common and crucial strategies for corporate security governance (Hu et al., 2021). Employees with slight cybersecurity threat awareness are considered easy objectives for cybercriminals; therefore, organizations need to implement security awareness through policies, procedures, and training sessions (Abu-Amara et al., 2021). Security awareness and training-centered objective involves reducing security incidents caused by system users.

The third component presented by NIST is data and information security. Confidentiality, integrity, and availability are an IT leader's three objectives for information security to protect and secure the data (Nasiri et al., 2019). These three factors act as the "pillars" of information security. Information security issues that can arise in information security management include unauthorized modification, illegal access, and interruption of IS (Chai & Zolkipli, 2021), in which ransomware threatens all three factors security-wise. IT leaders should develop IS practices that promote confidentiality, data integrity, and data availability. Ensuring adequate data availability can reduce ransomware impacts (Barker et al., 2022). The confidentiality factor restricts

the use and storage of various types of data, while the integrity factor guarantees that data will not be tampered with, as the availability factor focuses on giving access to the authorized user and related assets whenever needed (Chai & Zolkipli, 2021). Barker et al. (2022) recommend obtaining a data leak prevention solution and integrity-checking mechanisms to identify tampered software. Another strategy includes regular and scheduled testing of offline data backups for recovery and redundancy purposes (Barker et al., 2022).

The fourth protection component involves information protection processes and procedures. Top-level administration plays an essential role in information security organizational culture. A baseline of security principles and functions registers regular system use so that any deviation is treated as a tentative system threat (Barker et al., 2022). Security policies involve a "purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities…" (Barker et al., 2022, p. 12) There exists a need to encourage the implementation of cyber hygiene and information governance policies to healthcare professionals, as some may lack awareness of social engineering attacks such as spear-phishing (Nifakos et al., 2021), helping mitigate ransomware attacks. Processes and procedures allow for administering the protection of IS and assets (Barker et al., 2022). A robust organizational safety climate focuses on promoting employee safe behavior and compliance by implementing safety policies and procedures. Updating hardware and software and backing up systems should be part of a ransomware attack's response and recovery plans. Testing the HCO's backup, response, and recovery plans helps to understand recovery expectations in case of a

ransomware event (Barker et al., 2022). IT policy and security control for regular working patterns could include examples such as implementing a firm password policy, firewall protection, and preventing access to unknown emails and links (Muthuppalaniappan & Stevenson, 2021). Thorough auditing of health record systems access is a shared governance practice for HCOs. Other information security policies and controls for mobile devices containing personal medical information should include drive and data encryption, eliminating the possibility of installing unapproved software without consent, and securely connecting through a virtual private network when outside the network (Muthuppalaniappan & Stevenson, 2021). Restricting personal devices to organizational network access requires enforcement (CSRC, 2021). Network administrators should configure the antivirus software to automatically scan emails and flash drives and ensure blocking access to known ransomware sites (CSRC, 2021). Using standard user accounts needs implementation instead of administrative privilege accounts not to compromise login information (Padwal et al., 2019). It is imperative to conduct periodic vulnerability assessments that may present security deficiencies to improve (Padwal et al., 2019). Established data governance should include priorities for data policies, identifying roles and responsibilities for data privacy, security, confidentiality protection, and monitoring compliance on the information lifecycle (Padwal et al., 2019).

The fifth component presented by Barker et al. (2022) is the maintenance and repairs of industrial control and IS components. Industrial control systems include supervisory control and data acquisition systems, distributed control systems, and control system configurations like programmable logic controllers usually found in the industrial

sectors (Bhamare et al., 2020), including healthcare. Policy implements technical capabilities to mitigate cyberattacks on critical infrastructure (Scalco et al., 2021). IT leaders need to develop a long-term architectural policy to address the growing ransomware activity targeting the healthcare and public health sectors (Scalco et al., 2021). Maintenance and repairs must follow tested, proven policies and procedures, emphasizing remote maintenance while preventing unauthorized access (Barker et al., 2022).

The sixth and final component is protective technology. At its core, information security aims to protect organizational asset value. Information security management involves implementing and monitoring more than 130 security controls (Montesino & Fenz, 2011). IT leaders manage the security and resilience of systems and assets, configuring technical security solutions consistent with related policies, procedures, and agreements (Barker et al., 2022). Security controls reduce and mitigate asset risk, while technical controls or logical controls focus on hardware or software mechanisms to protect assets (Montesino & Fenz, 2011). Security control examples include policies, procedures, techniques, methods, solutions, plans, actions, or devices focused on helping secure the IS and infrastructure.

Technology helps organize the different security controls, techniques, and strategies that protect HIS from ransomware cyberattacks. Because organizations store essential business files with mapped network drives file servers when attacked, it causes a severe impact on business operations, as restoring system backups and system rebuilding takes some time (Karapapas et al., 2020). Endpoint protection is essential for HIS

cybersecurity as it assists in diminishing exploits in endpoint devices (CSRC, 2021). In many cases, compromised endpoints generate bypasses for remote launching ransomware attacks, so if servers try to prevent attacks using solutions, connected endpoints could still give way to the vulnerability through exploits located in the file server (Karapapas et al., 2020). To help mitigate endpoint infections, IT leaders can consider cloud infrastructure protection (CSRC, 2021).

Other technologies that help protect HIS include having an effective automated patch management system along with malware and antivirus protection to mitigate ransomware threats in healthcare (Muthuppalaniappan & Stevenson, 2021). Information security in HCOs can also be strengthened when IT leaders implement intrusion detection systems and intrusion prevention systems (IPS). The acquisition and implementation of security information and event monitoring (SIEM) software will identify associated events and monitor incident anomalies in real time (Padwal et al., 2019). Every network device needs monitoring service, including IoT medical devices (Padwal et al., 2019). A backup system application is crucial to fix affected systems through efficient file restoration (Reshmi, 2021). An autonomous backup system and plans are essential for stabilizing a healthcare IS' ransomware cyberattack (Reshmi, 2021). Quantitative risk analysis is a meaningful way to evaluate cybersecurity, but it lacks in most security programs of organizations (Kiser & Maniam, 2021). Tully et al. (2020) state that prevention and risk reduction for ransomware cyberattacks can be achieved with system user education, systems patching, and discontinuing unsupported software and devices.

A learning management system platform can help provide knowledge using learning modules focused on SETA programs for system users, employees, and stakeholders to educate on ransomware topics and maintain a history of employee professional development hours and effort (Padwal et al., 2019). A robust cybersecurity culture can fight ransomware through education and governance. SETA programs enrich information security culture (S. Kumar et al., 2021). SETA programs can change employees' behavior toward safer cyberculture, as cybersecurity awareness plays a vital role in cybersecurity (Lee & Kim, 2022).

Transition and Summary

The purpose of this pragmatic qualitative inquiry study involves exploring strategies IT leaders in HCOs use to protect IS from ransomware attacks. For the first section of this research, I presented the foundation of the study by establishing the background, business problem, research question, and theoretical framework. I also gave an overview of the research method, interview questions, and study significance seeking to provide the healthcare and IT industry with an extensive literature review along with a significant analysis of information to establish a scholarly study. The research literature review organized and sorted investigated topics to assist readers in internalizing the vast quantity of information presented in the study. The second section of this study focuses on precise details regarding adopting a pragmatic qualitative inquiry methodology to explore the strategies HCO IT leaders use to protect IS from ransomware attacks. Section 2 presents an all-encompassing description of the researcher's role, participants, populations and sampling, data collection, and research analysis. The third section of this

study presents the findings, applications to professional practice, implications for social change, recommendations for action and further study, author reflections, and conclusions.

Section 2: The Project

The purpose of this qualitative pragmatic inquiry study was to explore cybersecurity strategies some HCO IT leaders use to protect IS from ransomware cyberattack threats. The population for the study included IT leaders working in HCOs in the United States who had implemented cybersecurity strategies to protect IS from ransomware cyberattacks. The study's implications for positive social change include the potential to increase security standards that help protect IS and healthcare-sensitive information, including patients' PII. In this section, I discuss my role in the research, the participants, the research method and design, population and sampling, ethical practices, data collection instruments, data collection and organization techniques, data analysis, and the study's reliability and validity.

Project Ethics

Qualitative researchers play a central role in conducting their investigations. Qualitative researchers investigate issues in natural settings to interpret phenomena with the implications people present (Aspers & Corte, 2019). Qualitative researchers actively participate in collecting, organizing, and analyzing research data. Qualitative research emphasizes the subjective experiences and interpretations of participants, and researchers play an active role in exploring and interpreting these phenomena to generate insights and understanding (Aspers & Corte, 2019). McGrath et al. (2019) stated that the researcher acts as the primary data collection instrument in qualitative studies; therefore, I acted as a data collection instrument for this pragmatic qualitative inquiry research.

My professional background includes work in positions such as systems analyst and IT consultant, constituting a 10-year technical IT career experience. I also possess 15 years of academic experience as an IT professor and full-time university administrator. These experiences enabled me to complete my role as a researcher for this study. I have had information security experiences with ransomware and no prior connections or associations with the study participants.

Research efforts should minimize participant risks and maximize benefits for society (Hossain & Scott-Villiers, 2019). The *Belmont Report* (National Commission for the Protection of Human Subjects in Biomedical and Behavioral Research, 1979) describes basic ethical principles when conducting biomedical and behavioral studies involving human subjects. The *Belmont Report* presents three fundamental ethical principles that researchers must follow while conducting human research; respect for persons, beneficence, and justice. Respect for individuals requires that researchers provide participants with adequate information so they can voluntarily participate concerning their opinion in the study. Beneficence obliges researchers to treat them ethically while respecting and protecting their decisions. I adhered to and followed the *Belmont Report*'s ethics principles in this research. I completed the required human subjects research training (see Appendix A) and understand its importance to my study's requirements.

Pragmatist researchers consider that knowledge has specific and general functions that act together (Majeed, 2019). Qualitative approaches can implement strategies that address known sources of bias (Mackieson et al., 2019). For qualitative research, a

researcher plays an important step in the data collection process by acting as the instrument while gathering and interpreting data; therefore, neutrality and objectivity are necessary to curb research bias. These strategies strengthen the rigor and minimize potential bias, starting with reflexivity as it identifies the researcher's awareness of their influence on the phenomenon studied and how the research process affects them (Mackieson et al., 2019). As researcher and author of this study, I identified strategies that emerged from the participants' perceptions while using the interview data and documentation analysis. As a responsible researcher, I employed these strategies to maintain clean and unbiased research.

For this research, I identified and employed an appropriate interview protocol (see Appendix B) to improve research consistency. Interview protocols involve a succession of questions where participants express themselves on detailed subjects interrelated to the main research question (Jiménez & Orozco, 2021). An interview protocol offers a guide for each interview session (Ohn & Ohn, 2020). This semistructured interview protocol provided me with a revised script that included standardized open-ended questions for the participants to answer.

Informed consent is essential to human research (Fons-Martinez et al., 2022). Informed consent involves participants' voluntary participation with an understanding of what expectations their involvement implies (Xu et al., 2020). Research consent forms facilitate participants' trust in the researcher (Melis et al., 2022). Obtaining informed consent is fundamental to the adherence of ethical research principles that include respect, beneficence, and justice, according to Xu et al. (2020).

The consent form included text indicating to interviewees that they could withdraw from participation at any point during and after data collection (Lobe et al., 2020). I informed participants that they could avoid answering questions or renounce the study at any moment (see DeJonckheere & Vaughn, 2019). I disclosed procedures for participant withdrawal in the consent form and discussed them with the interviewees. If an interviewee decided to leave the research, they could do so at any moment without penalty.

Because cash incentives can increase the representativeness and number of individuals to recruit, it is an effective strategy to enhance recruitment in research (M. G. Smith et al., 2019). I offered a $20 gift card payment as an incentive to promote participation and as a token of appreciation for completing the interview and follow-up interview of the study. Millum and Garnett (2019) concluded that a gift card for an hour-long interview is not particularly coercive. Presenting the potential applied benefits of the study can act as an incentive for adults (Robinson, 2014); therefore, I will present the participants with access to a link to the published research.

Ethical issues addressed in any study include consent, confidentiality, anonymity, and data protection (B. G. Smith et al., 2021). I adopted all legal and ethical research requirements presented by the Walden University Institutional Review Board (IRB) to protect study participants' security. Adhering to the ethical research principles, I provided every interviewee with the informed consent form before each interview to ensure each individual understood the research's purpose and voluntary participation. I conducted the interviews taking into consideration the participants' voluntary participation and a suited

scheduled availability. According to Ibbett and Brittain (2020), four criteria help establish ethical safeguards in research with the author's acknowledgment of; formal ethical review by an IRB, participant consent was sought; participants were assured of anonymity or confidentiality, and that research is conducted utilizing a recognized ethical code of conduct. I followed these four criteria regarding the ethical safeguards for this research study.

Anonymity ensures the researcher that the participant cannot be identified from the study's data set, while confidentiality means that the participant's personal information will be accessed only as the participant authorized (Tiidenberg, 2020). Study participants were assigned a false name with the naming convention (P1, P2, P3, …) to protect the identity of the subjects. Names or other potentially identifying information will not be published, ensuring confidentiality and anonymity. PII was deleted from the transcripts securing patient privacy (C. Shi et al., 2020); therefore, I will do the same for this research. Only the researcher and Walden University's research committee have access to this study's information.

As part of the member-checking strategy, I asked for clarification responses during a follow-up interview. Member checking can help increase data saturation. The member-checking process allows data validation to ensure the source's credibility and confirm data accuracy (Zairul, 2021), following ethical research procedures. It is essential to gain participants' informed consent and address data security issues in qualitative online synchronous interviewing methods (Melis et al., 2022).

All audio and videoconference recordings and transcriptions of the participants' interviews was saved on an external hard drive which is locked in an electronic file cabinet inside my home office. Paper format data was also stored in an electronic file cabinet. The data set repositories need secure access, storage, and sharing of quantitative data (Antonio et al., 2020). The only people with access to the study's data are my dissertation committee and me. According to Klose et al. (2020), the *Menlo Report* suggests destroying data once past the retention period of scientific reproducibility. The gathered data will be secured for 5 years and then deleted and destroyed, as Walden University requires. Walden University's IRB approved this project (approval no. 40526401.)

Nature of the Study

This section of the research describes and justifies the research method and design utilized, deriving rationally from the presented applied IT problem statement. When researching a problem statement, the study's method and design need to be appropriate. The research includes quantitative, qualitative, and mixed methods as primary methods for research studies. The classification of an investigation is based on criteria such as the application, research objectives, and information being sought (Taherdoost, 2022) and the research's purpose (Kluge et al., 2019). This study follows a qualitative research approach after examining closely existing research methods and aligning it to the study's purpose.

Research Method

A qualitative research approach looks to disclose study participants' beliefs, ideas, feelings, and opinions about a central problem (Bleiker et al., 2019), generally expressed using words and not numbers (Busetto et al., 2020). Qualitative research methodology is more flexible and responsive, using interviews to collect text or visual images to provide rich sources of insight than the quantitative research methodology, which usually focuses on surveys to collect and analyze numerical data (Wolff et al., 2019). Through qualitative research, people's perceptions can be understood (Artioli & Sarli, 2021). This study explores the strategies that IT leaders in HCOs use to protect IS from ransomware cyberattacks; therefore, I selected the qualitative method as the most relevant research method. This research's purpose does not involve counting the amount of cybersecurity strategies used by interviewees but uncovering existing strategies. I opted for a qualitative method to seek an answer to the main research question. Qualitative research focuses closely on the human experience providing researchers with process-based, storied data on a phenomenon (Stahl & King, 2020). The main purpose of this research involves exploring the best strategies that HCO IT leaders use to protect IS from ransomware cyberattacks; hence I selected the qualitative research methodology.

When conducting quantitative research, sizeable random data samples are collected in a highly structured statistical format (Baur, 2019). The qualitative research method utilizes empirical statements and evaluation methods to describe statements by formulating facts of the investigated cases while analyzing the collected numerical data using mathematical methods (Taherdoost, 2022). As my research is not aimed at

enumerating or counting facts or figures associated with the central problem, quantitative methodology use is not a viable approach. Quantitative analysis involves systematic observation and description of properties of objects or events aiming to determine relationships between predictors as independent variables and outcomes as dependent variables in the studied population (Mohajan, 2020). Because my research does not involve correlating variables, I did not use a quantitative research methodology.

The main objective of this research involves exploring the strategies that IT leaders in HCOs utilize to protect IS from ransomware cyberattacks; therefore, mixed methods research does not align with the research objectives. The mixed methods approach blends the qualitative and quantitative data sets (Maarouf, 2019), viewing both as equal to respond to the study's research question (Dawadi et al., 2021). I did not apply the mixed approach to this research since it does not include quantitative components. The aim of this research involves gathering information based on the central research without collecting numerical data and not collecting numerical data for variable analysis; consequently, I did not apply a quantitative approach to this study.

Research Design

I applied a pragmatic inquiry research design to this study, also known as an interpretive description design. This approach provides the necessary tools to develop a deeper knowledge of the strategies that HCO IT leaders use to protect IS from ransomware cyberattacks.

Pragmatic inquiry research designs have been commonly used in qualitative data research as they represent an accessible and theoretically flexible approach when

conducting research in the medical education field (Tarikere et al., 2021). Interpretive description was born based on nursing epistemological grounds to produce usable knowledge for practice (Stevens et al., 2020). Interpretive description presents itself as an alternative research design because it can address complex experiential questions that generate practical outcomes (Tarikere et al., 2021). The pragmatic inquiry distinguishes interpretive description from other qualitative approaches while focusing on generating knowledge towards clinical practice (Stevens et al., 2020). The pragmatic inquiry approach produces an interpretive account created by probing through iterative and critical interrogation of a topic (Lapum et al., 2022). It helps the researcher understand the studied experience without surrendering the methodological integrity provided by qualitative approaches (Tarikere et al., 2021). Thorne's (2016) interpretive description methodology converts the collected data into patterns and reorganizing it into themes to answer clinical questions (Stevens et al., 2020). Characteristics, patterns, and structure can help process specific contexts to generate strategic paths to build knowledge through retroactive reflective interviewing, cross-sectional reporting, or longitudinal follow-up (Thorne, 2016). Therefore, this research validates the credibility of the study's findings using pragmatic qualitative inquiry.

Phenomenology studies a person's lived experience, searching to explain the experience's meaning according to what and how it was experienced (Neubauer et al., 2019). Phenomenological research design is often used in studies focusing on understanding the fundamental essence of the group's lived experience (Tomaszewski et al., 2020). The socially constructed reality of the participants of a phenomenological

study is provided through shared language and meaning. In phenomenological research, interviews are the primary source of data collection and may be supported by observations and personal diaries (Tomaszewski et al., 2020). A phenomenological research design was not feasible for this research as it does not focus on inquiring about personal lived experiences.

Ethnography involves studying social interactions, behaviors, and participants' perceptions through their eyes, time, and space during their living (Addeo et al., 2019). Ethnographic research is appropriate when describing how a cultural group works or exploring the shared lived group experience (Tomaszewski et al., 2020). Ethnography contributes to scientific generalizations about human behavior that are closely related to the functioning of social and cultural systems (Lai et al., 2019). Successful ethnographic research involves negotiation and renegotiation between the investigator and participants (Beckett & Kobayashi, 2020). An ethnographic research design is not appropriate for this research because I intend to explore strategies that HCO IT leaders use to protect IS from ransomware attacks, not researching the participant's cultural environments. Because this research did not require any type of investigation of a cultural group, an ethnographic research design did not fit the intended objectives of my study.

Data saturation is essential for sampling and enhancing qualitative data where study samples cannot be projected with assurance (Sebele-Mpofu, 2020). Data saturation happens when the researcher finds no newly acquired information from interviews or observations (Gill, 2020). It is used to determine when there is enough research data to build a solid comprehension of the research phenomenon (Hennink & Kaiser, 2022).

During data saturation, the researcher finds redundancy within the same findings in the data analysis process, signaling that data collection may be ceased (Islam & Aldaihani, 2022). I reached saturation when the (n+1)th interview did not present any additional data than the (n)th interview, as stated by Islam and Aldaihani (2022). To reach data saturation, I interviewed at least six healthcare industry participants individually. The sixth participant provided new information, therefore a seventh and eighth participants were interviewed. I added more participants until no further new information was identified from the data transcripts.

Population, Sampling, and Participants

The study's population involves IT leaders from the healthcare industry. Research sampling involved eight top-level IT leaders working in the healthcare industry in the United States. Purposeful sampling is commonly utilized in qualitative research for identifying and selecting information-rich cases about research issues related to the phenomenon studied by the researcher (Mohammadi et al., 2021). Studying information-rich cases yields insights and in-depth understanding rather than empirical generalizations (Mohammadi et al., 2021). Purposeful sampling assists in the selection of the participants enhances data gathering to support the responses and answers to the central question (Wolff et al., 2019). I recruited research participants using the snowball technique, as I asked participants at the end of the interview for new participant candidates. Before finishing the interview, I asked participants to nominate other participants for research participation (Armstrong et al., 2021). Snowball sampling is considered a valuable participant recruiting technique for qualitative research as it allows the investigator to get

to hard-to-reach populations (Armstrong et al., 2021). I selected purposeful and snowball sampling techniques for participant selection for this study. Identifying and selecting IT leader candidates as study participants requires additional attention and research on my part. Bautista et al. (2021) mention that the participants recruited through purposive sampling should be social media users that meet participant criteria. Participants recruited through snowball sampling involve participant referrals and social media profile access (Bautista et al., 2021).

Researchers consider data saturation the most popular guiding principle to corroborate the acceptability of data and rigor in a goal-directed sample (Guest et al., 2020). Saturation occurs in the data-gathering phase when no further insights are identified and data repeats, so additional data collection becomes redundant, indicating that the sample size was effectively reached (Hennink et al., 2019). Researchers suggest that sample size saturation ranges between 5 and 24 participant interviews (Hennink et al., 2019). Data saturation can be achieved in six to 12 interviews in qualitative studies (Braun & Clarke, 2021). Data saturation indicates that a sample is adequate for research robustness and content validity (Humayun et al., 2021). Saturation can be characterized by the themes' cumulative percentage of variability (Fofana et al., 2020). Saturation occurs when the (n+1)th interview does not present any new data than the (n)th interview (Islam & Aldaihani, 2022). The stopping point for an inductive study is determined by the researcher’s judgment and experience (Guest et al., 2020). To conduct this research, I selected at least six participants to conduct individual videoconference semistructured interviews and use inductive thematic analyses to decode the interview transcriptions.

Because the sixth participant described new information not presented by others, I interviewed a seventh and eighth participant. I added more participants until no new further information emerges from the inductive thematic analyses to decode the interview transcriptions.

Researchers view good participants as interviewees with lived experiences and knowledge on the subject of interest who are willing to be interviewed (DeJonckheere & Vaughn, 2019). To collect the required research information, I interviewed participants with knowledge and experience on the research subject and who are available to contribute to this research. Multiple participant criteria are needed to attain a homogenous sample (Waalkes et al., 2021). The participant selection criteria included: (a) participants who worked as IT leaders in HCOs from the United States, (b) for more than 5 years of experience, and (c) who had effectively applied cybersecurity strategies in HCOs to protect IS from ransomware cyberattacks. This selection criteria ensures that participants have the expertise to answer knowledgeably on this research topic. I filtered participant selection through location, job title, and IS experience.

The participant selection required detailed individual web searches through professional organizations and via social media for professional purposes, such as Twitter, Facebook, Instagram, and particularly LinkedIn Professional. Bautista et al. (2021) define social media in a research context as internet channels managed by users to generate and share resources through self-presentation to audiences that acquire value from that content. Therefore, using social media to locate possible study participants was critical for this research. Gaining access to participants through approved qualitative

methods helps establish research credibility. I used professional social media, email, and videoconference calls for this study to contact the participants.

I verified possible participants using selection criteria requirements. Before finding the names and email addresses of participants, I reviewed the job title to reflect their responsibility in the healthcare industry. I made the first contact with the interview candidates through social media messaging or email to send the invitation document (see Appendix C) with the informed consent form attached. I briefly presented myself, the research's purpose, and the consent. I established a working relationship with the participants to secure the best possible answers. Respectfulness of ethics and credibility will help generate plausible and trustworthy findings from participants (Stenfors et al., 2020). For the interviews, I established participant communication to clarify the research's purpose and present the possible benefits when applied to the healthcare IS, and to determine their interview participation commitment.

Building relationships and developing rapport are particularly emphasized for qualitative research (Novek & Wilkinson, 2019). Establishing a functioning relationship between the participants and the researcher will benefit this research. Xu et al. (2020) emphasized that information discussed with potential participants must fit their abilities and interests. Consent operationalization with a written and signed form is also key to establishing a working relationship (Xu et al., 2020). I will strive to create an atmosphere of openness, respect, and professionalism. Coercion, pressure, or influences can affect research results, therefore, must be avoided (Xu et al., 2020). Trustfulness will help me maintain in bond with the participants.

Data Collection Activities

My role as a researcher involved acting as a principal instrument for data-gathering techniques and analysis. Qualitative research researchers are often described as primary research instruments (Beckett & Kobayashi, 2020). Qualitative researchers use the inductive process to understand data, concepts, and theories (Mirick & Wladkowski, 2019). As the first instrument, the researcher analyzes the data, starting from the data gathering until the data report, while also planning, collecting, analyzing, and reporting the research findings (Rakhmawati & Priyana, 2019). When collecting the data, I paid attention to detail and searched for further explanation and subjectivity. I made sure that the required necessary data is collected to answer the main research question.

Busetto et al. (2020) stated that the conventional qualitative data collection methods are document study, participant observations, focus groups, and semistructured interviews. For this pragmatic qualitative inquiry research, I decided to utilize semistructured individual videoconference interviews to collect the data from at least six participants who are IT leaders from the healthcare industry. Interviews cannot be thought of as informal conversations with respondents by researchers because they are the data collection tools used to search for the research question's answers (McGrath et al., 2019). Researchers use semistructured interviews to collect new, exploratory data from a particular research topic, triangulate secondary data sources, or validate findings with member checking upon responding to feedback about research results (DeJonckheere & Vaughn, 2019). Semistructured interviews permit researchers to consult with the interviewees about what to talk about, significantly if the participant

deviates from the original theme, limiting the topic (Islam & Aldaihani, 2022). Interviews also permit the researcher to receive additional responses beyond specific questions (M. Johnson et al., 2019). Semistructured interviews create two-way communication between the researcher and the participant, promoting open-ended responses to gain more information on the study's topic (Islam & Aldaihani, 2022). The interview protocol and questions are located in Appendix B.

Interview protocols ensure that the questions follow the relevant topics while helping the interviewees stay focused (Lindgreen et al., 2021). Researchers should design interview questions to elicit deep responses from the subjects (Denton et al., 2020). My interview protocol was used during the data collection phase of this study, offering an overview of the interview process. The interview sessions lasted 30 to 40 min, as stated to the subjects in the protocol. The interview protocol was presented to the participants once they had agreed to be interviewed and recorded. I commenced the interview recordings by stating the participant's alphanumeric code, as well as the date and time of the interview. The interview protocol helped me structure and maintain the question's logical order, as presented in Appendix B. The interview's concluding section explains the concept and the overall plan. A follow-up to the question's responses clarified any doubts about my interpretation of the data presented. The interview protocol ended with a thank you message regarding the subject's participation. I sent the participant an email with a thank-you note and gift card information to thank the honoring of the invitation.

Qualitative researchers must also consider employing "socially distant" data collection methods (Lobe et al., 2020) as the current pandemic continues to affect society.

The researchers' and participants' health should be prioritized, particularly during the COVID-19 pandemic. During pandemics, face-to-face social interactions are forbidden and not encouraged (Melis et al., 2022). Because the nature of this study does not require physical contact between the participants and me, a videoconference semistructured interview collected a comprehensive set of data to answer the study's main research question.

Secondary data enriches the study's data collection process while accelerating the research time and cost of collecting more data (Renbarger et al., 2019). The study's literature review and the public sources from the industry found publicly on the web act as secondary data collection techniques. Secondary data documentation included documents from government agencies and industry-related agencies relying on available public resources (Kurniawati & Aliman, 2020). Collecting as much quality data as possible will help me obtain richer results.

Enhancing the reliability and validity of the data collection instrument and its process is significant to validate the study's rigor. Member checking also helps establish a study's trustworthiness by validating participant answers. Response validation is known as member checking (FitzPatrick, 2019). According to Rose and Johnson (2020), member checking is the most popular form of building trust in qualitative research. Member checking ensures that participants' contributions are accurately portrayed (FitzPatrick, 2019); therefore, every study subject had the opportunity to verify if the collected data exactly describes their views, experiences, and emotions. I achieved member checking by presenting the participants with summarized bullets of the interview results to verify my

accuracy. I coordinated a second interview with each participant to follow up on understanding the responses based on my summary of the research question answers.

Data Collection Technique

In this research, I explored the strategies IT leaders in HCOs use to protect IS from ransomware cyberattacks; therefore, I chose to conduct a semistructured videoconference interview as the most appropriate data collection technique. Data gathering was mainly based on online videoconference semistructured interviews, all of which were audio-recorded and transcribed. Qualitative research intends to produce a narrative understanding of a phenomenon of interest using data collection techniques such as interviews, focus groups, observations, and document analysis (Noyes et al., 2019). Interviews are considered the primary method of data gathering used in qualitative research, as they generate the most focused interaction between a researcher and the participants (Mahat-Shamir et al., 2021). During the interview, the interviewer engages in a conversation with the participant, trying to gain topic knowledge from the respondent through questioning and discussion (Husband, 2020). Different interview formats are available for use in qualitative research. The researcher's objectives shall determine the interview format to choose; structured, unstructured, and semistructured interviews (Mahat-Shamir et al., 2021).

Researchers can adapt videoconferencing platforms to qualitative interviewing techniques (Heiselberg & Stępińska, 2022). The COVID-19 pandemic has persuaded researchers in all disciplines to utilize online qualitative data collection techniques (Namey et al., 2022). There exists little or no difference between videoconferencing

platforms and face-to-face interviews in scientific research quality (Thunberg & Arnell, 2021). I employed a quality videoconference semistructured interview for these same reasons. To ensure semistructured interview quality, researchers should take on a relational focus, taking into consideration interviewing skills (DeJonckheere & Vaughn, 2019). Semistructured interviews should present easy-to-understand questions with open-ended, focused, and multi-dimensional questions within a logical organization (Koçoglu & Tekdal, 2020). I aligned the interview questions to be open-ended, fomenting conversation on the investigated topic of interest and searching for detailed revelations. The study's research questions were aligned with GST to provide a more logical structure. My previous interviewing experiences helped ensure quality for the semistructured interview as I followed the interview protocol with each participant.

I used a semistructured videoconference interview as a data collection technique, following a standard interview protocol of 10 open-ended questions (see Appendix B) related to the strategies IT leaders in HCOs use to protect IS from ransomware in the United States. An interview protocol acts as a guideline for interviews of probing and follow-up questions (Parfitt & Rose, 2020), providing structure to the data gathering process. After the participants' consent, the semistructured videoconference interview presented an overview of the study's topic. I was grateful to the participants for accepting the study's invitation. Afterward, I recorded the interview after they granted permission to record their answers. I asked the research questions once I received their consent. The interview duration lasted between 30 to 40 min. A second videoconference interview, lasting 15 to 20 min, ensured member checking. I observed member-checking by

discussing a bulleted interview transcription for accuracy and validity during the follow-up interview. Both the initial and follow-up interviews were recorded, transcribed, and summarized into a bulleted summary that accurately examined and verified with the participants. The interviews ended once I thanked the study participants and confirmed the participant's satisfaction with all question responses. Participants collected the gift card after their follow-up interview.

The interview data collection technique has various advantages and disadvantages. A significant advantage is that it can explore individuals' experiences, views, opinions, ideas, and beliefs on objects, issues, or phenomena (Islam & Aldaihani, 2022). Interviews help decrease data collection ambiguity and increase answer clarifications through member-checking, supporting the accuracy and validity procedures for the research's data gathering (Brown & Danaher, 2019). A semistructured interview is considered one of the most valuable techniques for rich data exploration because of its flexibility in communication (Islam & Aldaihani, 2022). Then again, the interview process can be time-consuming for researchers as questions were prepared in advance (Islam & Aldaihani, 2022). I focused on conducting the interview, working on the transcriptions, analyzing the collected data, searching for feedback, to report results (Brown & Danaher, 2019). Husband (2020) mentions three problematics for interviews; the interview setting can act as an artificial construct, participants are strangers, and the responses are limited to a time-restricted environment. Researcher experience is necessary to maintain high data collection standards, as participants may interpret the

research questions differently, presenting wide-ranging responses (Brown & Danaher, 2019). Appendix B shows the study's interview questions.

This qualitative pragmatic study collected data through interviews, analyzing and interpreting the data, validating my interpretations with the participants, who then confirmed or rejected the interpretations. During the member-checking process, the researcher asks the participants to approve or reject how the investigator interpreted the data (McGaha & D'Urso, 2019). Afterward, the interviews were recorded, transcribed, and summarized into a few bullet points. Participants were then interviewed for a final time, asking them to confirm or reject the summary of statements. I discussed the bulleted summary during a 15–20 min follow-up interview with the interviewees searching for the accuracy of their views. The second interview helped me correct any inaccuracies encountered. The member-checking process assists in the trustworthiness of the research (Souganidis et al., 2022).

Interview/Survey Questions

1. What cybersecurity strategies have you used to protect your healthcare organizations from ransomware attacks?
2. Have you participated in protecting information systems against a ransomware attack that accessed part or all the organizational healthcare information system (HIS) or patient health information (PHI)? Please describe this experience.
3. How do these ransomware attacks help shape current established cybersecurity strategies in your organization? Please describe the experience and elaborate on your response.

4. How do cybersecurity strategies fit into your organization as a whole?
5. How can you improve current cybersecurity strategies to protect IS better from ransomware cyberattacks?
6. What are the key barriers to implementing better strategies to protect IS from ransomware cyberattacks?
7. What are the frequent cybersecurity fail areas of IS guidelines & strategies regarding ransomware cyberattacks? Why?
8. What are the frequent cybersecurity success areas of IS guidelines & strategies regarding ransomware cyberattacks? Why?
9. What importance do external factors such as laws and regulations play in establishing cybersecurity strategies to protect IS from ransomware attacks in your organization? Why?
10. Which additional cybersecurity strategies would you implement to protect IS from ransomware cyberattacks? Why?

Data Organization and Analysis Techniques

Generating a clear organization system for qualitative data is essential for any research's success. Qualitative data management and organization techniques keep track of the study's data, ensuring it is appropriately handled and leading the investigation toward reliability and validity. In qualitative research, interview transcripts, audio recordings, and researcher notes need an organizing structure, which can provide a thematic analysis (Pell et al., 2020). Following that same line of thought, I used the same organizing structure for my study. I created a transcription of each interview utilizing the

cloud software Happyscribe.com. Then, I saved each record, preassigning alphanumerical participant names. Participant anonymity is essential in any research. A safe way to remain anonymous is to ensure that your real name or other directly identifiable information is not reported (Sim & Waterfield, 2019). I am protecting the participant's identities by distinctively designating the alphanumeric code where P1 and P2 respond to participants 1 and 2 correspondingly. I preserved a research log to record the research process, ideas, or situations experienced during the data collection phase. The collected data for this study was uploaded to the NVivo software to code identification of emerging patterns while storing data preserving participants' confidentiality. NVivo software helps the researcher identify and present the themes from the collected data. I have kept the study's data set files composed of the participant's consent replies, interview recordings, transcriptions, and public domain documentation in an encrypted file on a password-protected external hard disk drive for 5 years. When not in use, I place the external hard drive in a key-locked file cabinet in my home office. Once 5 years have passed since conducting the study, I will erase the digital information with a hard-drive format and destroy the remaining research documentation with a paper shredder.

I used a research log for my study as it is a valuable resource for idea correlation and thought arrangement that enables research topics and themes. Researchers maintain research logs to record the researcher's reflections (Miller & Flint-Stipp, 2019) and the study's work and understanding. Research logs can be used as a documentation tool for observations and relevant events, raising ideas, doubts, and thoughts from the study (Shalom & Luria, 2019). Research logs serve as a secondary piece of data to capture the

context of the study's data, granting an extra lens for data analysis and interpretation (Miller & Flint-Stipp, 2019), helping identify what still has not been discovered while assisting in capturing data and themes.

I decided to apply the multiple methods triangulation for this research from the four types of triangulation, as I analyzed various data collection methods. Triangulation ensures that the information from the study's data accurately reflects the truth about the investigated phenomena (Moon, 2019). Multiple methods triangulation occurs when the researcher utilizes more than one qualitative data collection method, such as interviews, observations, and documents (Natow, 2020). I used the data gathered from interviews and industry-related documents as part of the study's triangulation efforts. Triangulation will help increase the validity, reliability, and legitimation; while encompassing the research findings' credibility, dependability, confirmability, and transferability (Moon, 2019). Interviews will be combined with document analysis to form triangulation, as Mackieson et al. (2019) denotes that triangulation supplements and corroborates various data set findings to reduce research bias. Data analysis meets the rigor of qualitative inquiry through credibility, auditability, fittingness, and confirmability (Liang et al., 2020).

This qualitative pragmatic inquiry study explores the strategies HCO leaders use to protect IS from ransomware cyberattacks in HCOs. Data analysis assists researchers in understanding the gathered data. The researcher needs to engage in thorough qualitative data coding as it enhances the quality of the research analyses and findings (Skjott Linneberg & Korsgaard, 2019). The data analysis phase will examine the field notes and transcribed audio recordings that will later be coded and use qualitative data management

software (Busetto et al., 2020). This phase also involves document analysis, a valuable research method where books, articles, and other documents can be viewed as texts equivalent to the information a researcher collects during an interview (Morgan, 2022). The four factors to use when deciding what documents to analyze and include involve: authenticity, credibility, representativeness, and meaning (Morgan, 2022). Diverse industry and public documents focusing on information security on IS protection, including industry guidelines, policies, and procedures, were analyzed and compared to the interview notes. I stopped my document search when I gathered enough data to identify various themes, and exploring more data will likely not help me develop a new theme. Afterward, I wrote a report to connect each theme logically. Conducting a document analysis reduces ethical concerns associated with other methods (Morgan, 2022)

Researchers use transcript production as part of qualitative data analysis techniques (Vindrola-Padros et al., 2020). I analyzed the recorded interview transcriptions, field notes, and industry documents, searching to identify relevant themes and topics using NVivo software. The thematic analysis presents the participant's understanding of the experiences regarding the central research question. To analyze the gathered research data of this study, I will follow Sundler et al. (2019) three-phased thematic analysis method. The first phase of the thematic analysis involves achieving familiarity with the data through open-minded reading, followed by the second phase, which searches for meanings and themes, ending with the organization of themes into meaningful wholeness as the last phase (Sundler et al., 2019). Sundler et al. (2019)

thematic analysis method has been previously used in other studies, such as Shorey and Ng (2022) nursing research. During the first phase of thematic analysis, I identified the exact experience to study and limit personal bias. I used Happy Scribe cloud software to transcribe all participant interviews. Safarov (2021) and Kakadellis et al. (2021) have previously utilized Happy Scribe software to transcribe data research. I downloaded the transcripts from Happyscribe.com to Microsoft Word to reread the data to familiarize myself more with it. I also searched for logical meanings in the data to understand the participant's points of view. As part of the second phase, I identified the differences and similarities between definitions while searching for patterns using the transcriptions in the NVivo software. The NVivo software identified repetitive statements, words, or phrases.

For the third phase, I organized the identified themes into whole and meaningful text. Because themes emerge from word patterns, it is crucial to make sure that the explicit naming of the themes describes the meanings of the experiences (Sundler et al., 2019). Thematic analysis helps the researcher analyze interview data to detect patterns called themes (Karavadra et al., 2020). Using a determined naming convention, I created and used labels to set apart each theme and information about that theme. As part of the analysis process, I considered the GST conceptual framework as an additional viewpoint to analyze the gathered research data. I viewed the major themes through the lens of the GST conceptual framework allowing me to address the research questions about protecting IS from ransomware attacks in HCOs.

Reliability and Validity

Researchers can obtain a study's rigor through dependability, credibility, transferability, triangulation dependability, and confirmability (Coutts & Solomon, 2020). A researcher can safeguard the reliability and validity of qualitative research. Research reliability embodies the dependability or consistency of research data analysis (Chan & Chen, 2022), as it is fundamentally demonstrated by data triangulation (Quintão et al., 2020). Research validity embodies the truthfulness of research data analysis (Chan & Chen, 2022). Drawing on this, I provided concise notes on decisions taken while researching, utilizing research materials, sampling, and emerging data management outcomes.

Dependability

To ensure dependability, the researcher must report the research method in detail so the reader can verify the best research practices and future researchers can replicate the investigation (J. L. Johnson et al., 2020). Because dependability is an alternative notion to reliability in quantitative research (Nassaji, 2020), I provided a concise note set providing the decisions taken while conducting the study, as well as the use of research materials and study findings.

Member checking was employed and considered in this research. Member checking provides data rigor to research (Hayat et al., 2021). Member checking was accomplished through a follow-up video-conferenced interview, where participants were given summarized bullets of their answers to validate the answers' accuracy and

dependability. Bhuyan et al. (2020) state that member checking provides authenticity to study results.

Credibility

In qualitative research, credibility occurs when study conclusions can be viewed by researchers as credible, concerning the accuracy of results upon the reality of the phenomenon investigated (Nassaji, 2020). Reliability is identical to credibility (Collingridge & Gantt, 2008). To achieve credibility, I ensured an understanding of the research participants, context, and processes for accurate analyses. Because triangulation uses multiplicity to assess the credibility of a study (Stahl & King, 2020), it played an essential role in this study's data analysis and results. Walden University's IRB process approval also contributed to the study's credibility.

Transferability

Ferrando et al. (2019) define transferability as the level to which findings can be generalized or shifted to other contexts. A researcher considers a qualitative study transferable if the results have meaning to individuals not involved in the investigation or if the research readers can relate the findings to their own experiences (Daniel, 2019). For this study, I provided a complete account of my research experiences, including details on the data collection process and research practices. I promoted research transferability through context explanations and assumptions.

Confirmability

Confirmability is parallel to objectivity in quantitative research (Nassaji, 2020). Research confirmability searches to reduce study results influence by employing rigor

standards like triangulation, member checking, and peer review (J. L. Johnson et al., 2020). Confirmability has to do with other researchers confirming the research interpretations and conclusions (Nassaji, 2020). To obtain confirmability in my study, I generated transparent and detailed descriptions of this research's data collection, analysis, interpretation, and methodologies. I also provided a detailed description of the integrated methods for seeking participants' perceptions regarding validity and conclusion. Every participant received a bulleted summary of the essential points of the interview to promote accuracy while bracketing, and the member-checking development will help with the study's objectivity. Liang et al. (2020) mention that bracketing eliminates preconceived notions as it helps focus on understanding participants' answers, supporting to ensure data collection and analysis validity while maintaining the study's objectivity.

Data Saturation

Data saturation occurs when no new themes appear in the participant interviews (Guillain et al., 2020). It is essential as it implies stopping the data collection process (Farrugia, 2019). For this research, three sources of information helped achieve triangulation: interview results, interview observations, and IT industry documents publicly available on the internet. This study reached data saturation by interviewing a second participant and comparing the conclusions of the first two interviewees to ensure they aligned with related information. If I found no similar statement, I proceeded to interview a third participant, followed by other participants, until new information was revealed. After, I verified saturation within each interviewee, I compared the interview responses. If I detected similarities in the data collection analysis and no new data was

gathered, then saturation was achieved, ending the data collection phase. I contacted additional participants if statements that any one participant made were not corroborated by at least one other participant. According to (Wainwright et al., 2019), data saturation happens when researchers cannot identify new themes in the research process, helping determine the sample size and aiming for data richness that fulfills the research's goals. Researchers must show evidence of how they reached data saturation in their study (Gill, 2020).

Transition and Summary

The purpose of this qualitative pragmatic inquiry study was to explore strategies that IT leaders in HCOs use to protect IS from ransomware attacks. Section 2 of this research presents the study's primary purpose, participants, techniques, data collection methods, analysis, and organization, as well as population and sampling, following ethical research strategies. Section 2 presents the target study participants, which involves IT leaders working in HCOs in the eastern United States. I gathered data while conducting semistructured interviews through videoconference to undergo a thematic analysis which includes analysis of field notes. A document analysis of industry-related documents helped validate the study findings through triangulation. I focused on the result validation of this qualitative pragmatic inquiry study by addressing the dependability, credibility, transferability, confirmability of the data analysis, and data saturation.

In Section 3 of this study, I provided the research findings of IT leaders' strategies in HCOs to protect IS from ransomware cyberattacks. Section 3 presents the application

to professional practice, implications for social change, recommendations for action and further study, reflections, and a conclusion statement. I connected the study findings to the conceptual framework of my research by discussing examples given during the interview by the participants.

Section 3: Application to Professional Practice and Implications for Change

The purpose of this qualitative multiple case study was to explore the strategies that healthcare IT leaders use to protect HIS from ransomware cyberattacks in the united States. Three major themes were revealed during the thematic analysis phase of the research. Evidence from the interview data addresses security management practices, as the first major theme, and as one of the most significant strategies to protect IS from ransomware. Security management practices refer to a set of systematic, technical, strategic actions and tools that IT leaders put in place to protect organizational information assets and technology infrastructure from security threats and vulnerabilities. The security planning elements theme emerged as the second significant theme from the thematic analysis applied in the study. Security planning is a critical aspect of information systems security, as it involves developing a structured approach to safeguarding and protecting information systems. Effective security planning helps organizations establish governance, security policies and procedures, while allocating resources to protect sensitive data and systems. The third major theme involved the human element of information systems. The human element is a critical aspect of information systems security, as people play a significant role in both safeguarding and potentially compromising an organization's data and systems. Human elements encompass the actions, behaviors, and decisions of individuals within an organization.

Presentation of the Findings

The main research question that underpinned this study was, What strategies do healthcare IT leaders use to protect IS from ransomware cyberattacks? To answer the

research question, I conducted semistructured interviews to gather data from healthcare IT leaders who had been involved in strategies to protect HIS against ransomware cyberattacks in the United States. Eight IT leaders consented to participate in the interviews. All eight participants were given a alphanumeric code (e.g., P01 for Participant 1, P02 for Participant 2), for anonymity and confidentiality purposes to protect their identities. I conducted follow-up reviews with the research participants to verify the transcript summary data as part of the member-checking process.

I also collected 10 industry documents (e.g., ID01, ID02, ID03) related to ransomware attack protection for literal triangulation purposes, which are displayed in Table 1. In literal triangulation, information is gathered from only one source, in this case an interview, and is verified in exact terms to another source, such as information security industry documents, to verify consistency to indicate validity and credibility in the research description construction process, providing confidence in the research's outcome (Sridharan, 2021). Tables 2 through 4 show the data collection references used in the study findings. I uploaded the member-checked interview transcripts and 10 industry documents into the NVivo 1.71 application to analyze the collected research data.

The study's findings present healthcare IT leaders use different strategies to protect HIS from ransomware cyberattacks. The thematic analysis presented three main themes from the NVivo software data analysis: (a) security management practices that include technical defense practices as well as protective technology tools and solutions; (b) security planning elements including governance, procedures, and policy; as well as (c) the human element focusing on security training and security awareness arose as main

research themes through code interpretation. After discovering the main themes, I was able to link the thematic analysis to the research's literature review and conceptual framework.

Table 1

Industry Documents

Document ID	Author	Title
ID01	Cyber Readiness Institute	*Ransomware Playbook: How to Prepare for, Respond to, and Recover From Ransomware Attack*
ID02	Cybersecurity and Infrastructure Security Agency	*Protecting Against Ransomware*
ID03	Cybersecurity and Infrastructure Security Agency	*CISA-Multi-State Information Sharing and Analysis Center (MS-ISAC) Joint Ransomware Guide*
ID04	Information Systems Audit and Control Association	*Ten Ways Hospitals Can Prepare for Ransomware Attacks*
ID05	Information Systems Audit and Control Association	*To Pay or Not to Pay: Proven Steps to Ransomware Readiness*
ID06	Microsoft Support	*Protect Your PC From Ransomware*
ID07	National Institute of Standards and Technology	*Getting Started with Cybersecurity Risk Management: Ransomware*
ID08	National Institute of Standards and Technology	*Tips and Tactics: Preparing Your Organization for Ransomware Attacks*
ID09	Pompon, R for F5 Labs	*Cybersecurity Controls to Stop Ransomware*
ID10	Snoke, D., T., & Shimeall, T., J. for Software Engineering Institute	*An Updated Framework of Defenses Against Ransomware*

In the subsequent sections, I present an in-depth examination of each thematic element alongside the perspectives articulated by the participants involved in the study. Furthermore, a comprehensive exploration of the three primary themes, as identified in

the thematic analysis stage, is conducted concerning pertinent academic investigations, GST as the conceptual framework for this research, and the implementation of effective IT strategies to protect HCOs from ransomware cyberattacks.

Theme 1: Security Management Practices

Security management practices were the first significant theme to arise from the study's data analysis stage. Security management practices encompass the evaluation of organizational resources, including the development, implementation and documentation of cybersecurity policies, controls, and procedures to ensure optimal safety of the assets. Given the ever-changing and intricate ransomware landscape, IT leaders must adopt a proactive cybersecurity approach to combat ransomware cyberattacks, maintaining a current vision on emerging threats, vulnerabilities, and risks. The surge in ransomware attacks targeting HCOs underscores the importance of employing the right combination of cybersecurity tools and management practices to defend information systems from these cybersecurity threats. Consequently, the successful deployment of best technical defense practices combined with the right technical security tools and solutions, can effectively thwart a ransomware cyberattack. Table 2 illustrates the quantity of references pertaining to theme of security management practices.

Table 2

References to Security Management

Major theme (subtheme)	Participants		Document	
	n	No. of references	*n*	No. of references
Security management practices	8	168	10	67
Technical defense practices	8	89	10	37
Protective technology tools	8	79	10	38

Findings From Participant Interviews

All eight study participants specified using security management practices to protect information systems from ransomware cyberattacks. P01 mentioned, “So, there's technical defenses...so we've protected our perimeter with different technologies that will deter attacks or detect attacks and then respond automatically.” P01 also stated, “So, there's establishing the technical defenses, and then we test those technical defenses to make sure that they work.” Following that same line of thinking, P03 indicated, “My strategy is always to really put in the basics of technical controls.” In the same vein, P05 mentioned as well “…when we talk about the success areas, it's more about putting all the controls in place.”, referring to the technical controls.

Technical Defense Practices. Technical defense practices are a critical component of ensuring the security and integrity of our organization's digital assets. These practices involve deploying and managing a range of technical measures to protect against cyber threats and vulnerabilities. These include identity management, network management, vulnerability management and technical control testing. Table 3 illustrates the quantity of references pertaining to the topic of technical defense practices.

Table 3

References to Technical Defense Tools and Best Practices

Subtheme (secondary subtheme)	Participant		Document	
	n	No. of references	*n*	No. of references
Technical defense practices	8	89	10	37
Identity management	8	28	9	9

Network management	7	39	4	14
Vulnerability management	5	12	9	13
Technical control testing	5	8	1	2

Identity Management Practices. All eight of the participants used technical defense practices to protect IS from ransomware cyberattacks, assigning it as the first subtopic. All participants mentioned using identity management controls focusing on access control and account control. P03 stated that "Bad actors are compromising an account, going out and injecting malware, and or locking out a privileged account." The same participant also mentioned that "…killing a few birds with one stone, on that is looking at how we can put on proper access management, risk-based MFA, with more minimal access and everything to that." P03 continued mentioning "So, if you're looking at that, you look at all the accounts, that can do most harm to your organization, and you do privilege access, and you put additional monitoring on that." P01 mentions "Eventually we rolled out multifactor authentication for all remote access. Following that same line of thinking, P06 stated, "We have two factor authentication." P07 stated that "The fourth implemented strategy would be implementing things like privilege or identity management controls." P05 mentioned that protection lies in "taking controls from the end users really onto the servers or onto the core engine, so that the users have less and less control with them and all the things are really governed on the back end." Following that same thought, P04 indicates "We segment security in terms of accounts, so people have only regular user; for example, as an admin, you only log into your admin account only when you need to do admin stuff. Otherwise, you are a regular user." P02 presents the importance of strategically implementing account control with other strategies such as

network management by stating, “I think that not enough people using web proxies, not enough people microsegment, a lot of people punt on the account control and disabling, not even knowing what all the accounts are.”

Network Management Practices. Seven out of the eight participants mentioned network management as part of the technical defense practices of security management. Network management in information security refers to the set of processes and practices designed to ensure the availability, integrity, confidentiality, and optimal performance of an organization's network infrastructure while effectively mitigating security risks. Network traffic filtering as well as network access, integrity, and confidentiality emerged from network management. Five out of the eight participants mentioned network segmentation and segregation as an essential defense technique to maintain network integrity. P02 stated “So, in this case, we can talk about how the segmented network was a good strategy for working out the situation of the ransomware attack, especially right when it started.” In that same line of thought, P02 also stated. “So, you think about micro segmentation, it mitigates impact and potentially frequency (of ransomware).” P04 acknowledges using network segmentation when expressing, “We segment the network, and we make sure that people only have access to the things they need to have access to.” P07 explains that “…just segregating so that if something is at large in your environment, you're increasing the friction for it to jump a network boundary or firewall.”

P01 mentioned the following statement regarding medical devices that “From the external environment, we do scans of the devices that are in our environment to determine what the vulnerabilities are and that they are all on the segregated part of our

network where less harm can be done." The same participant continues stating that "Medical devices can present security challenges." P05 mentions "We have to do all the integration of the devices with IoT medical devices, like cardiac monitors. We try to bring all those devices into one umbrella. That is a difficult task to do because of proprietary things." P05 goes on to mention that "Then we have some zones. Who can log in? From which zone? Which area? If they are connected to some from other zones, we are restricting that." Medical devices can have some update limitations, but segregation can help take care of that as stated by P01,

> In healthcare, we have a specific challenge with devices that cannot be updated because they require FDA approval. And those are a pretty well-known sort of weak spot in our armor. So, for those, these are medical devices that are typically running a Windows OS. And if you cannot patch it because the FDA says it is only approved for patient care up through this patch level, you have to leave it there even if there is a known vulnerability. So, there we do some network segregation so that if a device does become compromised, it cannot be used as a steppingstone to get into the rest of our network.

Five out of eight participants mentioned various network traffic filtering defense techniques. Network inbound and outbound filtering are security measures designed to control and manage incoming and outgoing data, requests, and network traffic within an organization's network. These filtering practices help enhance network security by allowing or blocking specific types of traffic based on predefined rules and policies. The geofencing practice was presented as an inbound technique by P04, as the IT leader

stated “Another thing is geolocation systems. A lot of systems now have the ability to block where things are coming from and to be able to block things.” The same participant continues indicating “So, we use systems where our firewalls block traffic coming from just about anywhere but the United States, depending upon what organization it is and where they do business.”

In that same vein P01 stated, “We figured out that the people that were doing this were coming from overseas, so we started blocking access from different countries based on their IP [internet protocol] address.” P02 expressed using outbound filtering and then focus on extensive controls of the web channel outbound to try to pick off any potential malicious sites.” Firewall use and configuration help maintain network security. P05 stated,” Then the other thing, we have everything behind the firewall, and we have the failover, and these are next generation firewalls that do give us this protection.” P05 goes on and indicates, “Obviously, onto the back end, then there are multiple layers of security, especially putting those things behind the firewalls, especially intelligent firewalls.”

Vulnerability Management Practices. Vulnerability management is also an important defense practice against ransomware. Vulnerability management is the systematic process of identifying, assessing, prioritizing, and mitigating security vulnerabilities within an organization's systems, applications, and network infrastructure to reduce the risk of exploitation. Five out of eight participants mentioned vulnerability management as a ransomware protection strategy. System updates and security patching emerged as key elements in vulnerability management. P03 mentioned “Vulnerability

management is super important." P07 mentioned that "The third strategy was things like vulnerability management." P01 directly mentions the use of system updates stating, "We do updates every month and take the systems down. So, people have lots of experience working without the systems. Like, you know, we get these updates done in less than 2 hr and we do it at night." P06 follows the same line of thought stating, "The tactical controls that can help you prevent ransomware from occurring, is doing the basic hygiene of patching and things of that nature. So, if you think basic hygiene, you think about patching machines, keeping your systems current." P08 mentions that "Every device needs to be maintained to current version of an operating system."

Technical Control Testing. Technical controls should be tested periodically to ensure they are working on protecting the data. P01 indicated that "Once a year we will do an actual penetration test where we hire white hat hackers to see if they can get in. Part of their examination involves technical defenses to see how they work within protecting the perimeter." P07 also recommends periodic penetration testing as the participant stated, "So, most organizations have a very robust ransomware response plan and you're exercising as you're going through penetration tests."

Protective Technology Tools and Solutions. The second subtopic for security management practices is protective technology tools and solutions. Protective technology tools and solutions in IT refer to a range of software, hardware that are employed to safeguard an organization's digital assets, networks, and systems from various security threats and risks, in this case from ransomware cyberattacks. All eight participants noted having protective tools and solutions in place against ransomware as shown in Table 4.

Table 4

References to Security Management Tools and Best Practices

Subtheme (secondary subtheme)	Participants		Document	
	n	No. of references	*n*	No. of references
Protective tech tools and solutions	8	79	10	30
Email protection	7	18	3	5
Endpoint protection	7	14	2	3
AI	6	14	0	0
Backup protection	5	14	7	14
Other subthemes				
Antivirus protection	3	3	3	3
Security information and event monitoring	2	2	1	1
Extended detection and response	2	3	0	0
Disaster recovery system	2	2	0	0
Intrusion prevention and detect	1	2	2	2
Data loss protection	1	4	0	0
Vulnerability detection and response	1	1	1	1
Vulnerability detection and response	1	1	0	1

Email Protection Practices. Seven of the eight participants mentioned an email protection tool. P01 mentioned, “We use tools that are looking at all of the email traffic that's coming in and scanning the email to see if there's a malicious payload attached to anything that's coming in.” Regarding the same thought, P02 mentions that “Security starts with inbound filtering, particularly on email.” P02 also states that “…in the case of email protections, you are really diminishing the frequency because you're making it more difficult for the attack to begin with at all.” P06 stated that “email threat protection is really tactical control that can help you prevent ransomware from occurring.” P08 mentioned, “One of the things I would do is I would look at tool sets that look at content of email and block based on content.” P05 stated, “Even with having all those email

security policies at a high level, still bad emails come into the inbox." The same participant continues mentioning "But sometimes, mostly that scene that email is coming, it looks like it is coming from Microsoft to change your password, and it's a scam." Therefore, we need to implement other security strategies as failovers to phishing scams as phishing is considered a threat vector. P06 validates this thought stating, "Working with other executive leaders in the business for them to better understand what are the main threat vectors that ransomware is coming in from, and that being phishing." P08 also mentioned "Most ransomware attacks do originate, in my experience, through email."

Endpoint Protection Practices. P07 indicated that "…getting into phishing proof protection is important." Endpoint protection system is another tool presented by the participants for the protection against a ransomware cyberattack. P02 mentioned that "HCOs got to have EDR [endpoint detection response] or some other type of high-fidelity EDR." The same participant stated, "So EDR and XDR [extended detection and response], I think, have taken off like a rocket ship. And so, I think particularly in the regulated workspace is very common." P06 mentioned that "…when you get into the more technical and tactical perspectives, you really are trying to ensure that you have the protections in place to show reasonable security in the sense of endpoint protection." P08 stated "Having a tool like Intune from Microsoft on every device would allow me to allow or disallow access and manage how much access based on not just user identity, but also device, which would be hugely beneficial towards a future direction." P03 stated

that "…endpoint systems can give more forensic viability to see if there's compromised components of files."

Artificial Intelligence Protection Practices. AI tools can play a significant role in protecting information systems from ransomware cyberattacks by providing advanced threat detection, prevention, and response capabilities. Six out of eight participants mentioned AI tools for information systems protection. P02 indicated "So, I'm a big fan of this notion of omnipotence knowing all time on all system, everything going on, but when you come to the processing side of that, you got to have machine learning and AI." In the same tone, P03 mentions "We're starting to look to then put in some more overlays of AI technology to really help end user behavior and doing more insider threat monitoring of privileged users and or high-risk users." The same participant stated "There's no silver bullet from a technology view, but there is a lot of cool stuff that is on the way on artificial intelligence. So, you should embrace it to look at user anomalies." P04 sees AI as an effective tool as the participant states "Some of the more effective systems now are using AI, like the systems I mentioned before, they are using AI to try and figure out, hey, if something is going on, I isolate that machine. "The same participant continues mentioning that "There is an AI process that is taking place. From what I have seen, they are very effective." P05 implemented AI based firewalls, and the participant indicates that "Right now, we are putting all those AI based firewalls. Those are really reading all the signatures of the traffic. Based upon those signatures, those can really, at their own, they can identify any suspicious traffic." P06 follows the same line of thought expressing "So really making sure the behavior analytics technology, machine

learning, so on, so forth is in place to really detect ransomware inside the system." All participants use three or more protective technology tools & solutions and have expectations of implementing more in the future, particularly AI based solutions. P08 stated that because cybersecurity has large quantity of data, AI is there to help analyze it by stating, "…AI us the future. You cannot go through any interview or any discussion of cybersecurity without at least saying it. I think this whole cybersecurity problem really is a big data problem. It is a massive amount of data." AI and machine learning can help manage large amounts of data and help detect unauthorized data movement while analyzing user behavior as well.

Backup Protection Practices. A backup solution tool is software or a system that automates the process of creating duplicate copies of an organization's data and storing them in a secure location to protect against data loss, disasters, or system failures. Backup solution tools typically include features such as scheduling backups, version control, and options for on-site and off-site storage. Five of the eight participants mentioned backup protection using a protective tool and solution. P08 mentions "Backup recovery is a protective tool." The participant continues stating that "Having an image for every application, making sure every application is maintained to current version is very important." P08 also mentioned that it is of utmost importance "Having an image for every application, making sure every application is maintained to current version." P01 mentions that backups help us go back in time by stating "Backup strategy has changed over the last 18 months. We now have 13 months of unalterable backups so that we can restore to at any point in the last 13 months." The same participant mentions the

importance of having more backup time by mentioning “If somebody is able to get in, we may be backing up ransomware that has a long fuse on it, so we have to be able to go back in time.” P04 was involved in a ransomware attack and stated, “We were fortunate that we had a backup. We had a partner that was an MSP that worked with us and got them involved because we wanted to make sure that somebody really knew what they were doing.” The participant went on mentioning “They had seen this before, so they knew. They carefully cleaned the network and got rid of it so it would not come back. Then they helped us restore the files from the backup.” P07 mentions that “We're seeing hospitals fail with their backup mechanism.” An example arises from P08s following comment, “We did have backups, which we were able to recover, except for parts of one system where, without getting into too much detail, part of the system wasn't backed up properly, and so we lost some historical data.” Definitely backup testing and backup experience are security management practices to take into consideration when protecting IS from ransomware.

Other Protection Tools and Practices. Three of eight participants mentioned the use of Antivirus protection. P06 mentioned, I have got three virus scanners running in my workstation right now.” P08 mentioned that “the thing I was trying to do is apply an Antivirus.” Two of eight participants (P01 and P02) mentioned using a SIEM solution, with P02 expressing the need for “network monitoring that allows you to do forensic as well as detective.”. P02 presents two other tools and solutions that help protect IS from ransomware by stating “And a number of endpoint controls to look for, should those fail, some type of malicious payload beginning to activate AV (access violations) is not very

effective." The participant added, "The EDR and XDR—all the DRS [disaster recovery systems]—now tend to close the gap of that visibility and then both a midpoint collection as well." P02 also mentioned IPS: "Again, various detection and prevention capabilities from a host based EDR kind of host based IPS or east-west, and then shutting down all that really becomes a denial permit by exception, even on the internet." The use of technical defense practices along with protective technology tools help protect IS from ransomware, but it depends on other information security strategies as well. Following on this same idea, P08 stated, "It is probably in the current state with technology controls, it's a good idea because technology controls don't catch all, and that's probably going to be the case for a while."

Findings From Industry Documents

Industry documents' evidence supports information security management practices as an important cybersecurity protection strategy theme against ransomware. All 10 industry documents reviewed identified specific defense practices against ransomware that were employed by HCO IT leaders. ID1 focused mainly on technical defenses involving vulnerability management and backup protection as protection strategies against ransomware. ID2 recommended vulnerability management such as updating and patching systems as well as using protective technology tools such as email protection and backup protection. ID3 presented practices such as identity management, network management, vulnerability management and technical control testing. This document also supported the use of protective technology tools for email protection, antivirus protection and the use of intrusion prevention & detection system. ID4 promotes

the use of security patching as a technical defense practice as well as the use of protective technology tools to protect IS from ransomware. ID5 focused on using a protective technology solution for endpoint protection. ID6 mentioned vulnerability management such as system updates, backup protection practices and the use of an antivirus tool as effective countermeasures against ransomware. ID7 presented identity management defense practices as well as network management practices for network access including segmentation and segregation the network as IS defenses. Security patch management as well as technical control testing were also presented as strategies to protect IS from ransomware. The use of technology solutions for endpoint protection, backup protection and use of a SIEM were also mentioned by ID7. ID8 validated the use of access control defense practices, network access management, security patching and use of an antivirus solution as protection cybersecurity practices. ID9 shows as technical defense practices the use of identity management, network segmentation, network monitoring, vulnerability management, and backup protection. ID10 focused on the use of network traffic filtering and vulnerability management as technical defense practices. It also focused on having a protective technology solution for email protection, backup protection and intrusion prevention system. Industry documents present existing security strategies to be implemented by HCO IT leaders to protect IS from ransomware cyberattacks. Data presented by the industry documents confirm the research participants' perspectives.

Connections to Effective Information Security Practices Found in the Literature

The perspectives of the interviewed participants on the importance of security management practices align with current literature. As stated by Brunner et al. (2020),

information security management practices consequently deal with the implementation and monitoring of an organization's desired information security level. Eight out of eight participants implemented and managed some form of security management practices to protect HCOs from ransomware cyberattacks. According to Pérez-González et al. (2019), information security within organizations reveals a shift in information security management, transitioning from technical perspectives to more managerial approaches. This study identifies both aspects as an integral strategy to protect IS from ransomware. Initially, the earliest references exploring information security in corporate settings predominantly centered on describing it from a technological standpoint and searching for technical solutions to enhance it (Pérez-González et al., 2019). In this study, eight of the eight participants mentioned at least three technical defense practices each implemented in their HCO to protect IS from ransomware, highlighting the importance they have on protecting IS from ransomware. Technical defenses such as file access, access control, email protection, and backup controls (Alshaikh et al., 2020) provide IS ransomware protection. Also, eight of the eight participants used more than two protective technology tools and solutions to protect IS from ransomware cyberattacks. It is estimated that 25% of infected PCs have antivirus installed, indicating that these applications alone cannot prevent infections from happening (Uandykova et al., 2020). More technological tools are being implemented along with the use of AI to have better analytics of user behavior and network monitoring. New generation programs complement signature-based detection and modify programs' monitoring behaviors becoming more specific at ransomware threat detection (Du et al., 2022).

Connections to the Conceptual Model and Other Studies

The preceding section of the study ties the theme of security management practices to GST's conceptual framework of this study and other existing published research. GST follows a holistic approach, meaning it views the system working in coherence as a functional unit. GST approaches systems problems within stated boundaries (Turner & Baker, 2019). The whole system defines and determines the part's roles as the entirety surpasses the mere summation of its constituents (von Bertalanffy, 1968). Healthcare IT leaders use security management practices to establish and maintain different technical defense practices while implementing protective technology tools to protect IS from ransomware. Because HCOs are composed of many different interrelated areas and systems, it creates a unique technological landscape challenge against ransomware risks and increasing threat vectors. Systems delineate spatial and temporal boundaries that encircle and impact their interaction with the environment, all the while being defined by their structure and intended function (CUI Weicheng, 2021). Through security management practices HCO IT leaders can view through the GST lens a bigger security picture helping identify tools and practices holistically to reduce the risk of a ransomware cyberattack.

Theme 2: Security Planning

Security planning was the second significant theme to arise from the data analysis phase of this study. Information security planning is a critical component of any organization's strategy in today's digital age. Every organization should have appropriate information security planning and governance methods to protect information systems

(Ranganath & Rajeshwaran, 2022). It refers to the systematic and proactive process of safeguarding an organization's information assets from different threats, including cyberattacks, data breaches, unauthorized access, and other forms of harm. Information security planning involves the analysis of threats and consequences by location and source in an organization (Andrzejewski, 2019). A well-structured information security plan is essential to mitigate information security risks and ensure the confidentiality, integrity, and availability of critical data. The security planning theme is divided into the following subthemes: governance, security procedures, security policies.

Table 5

References to Security Planning Elements

Major theme (subtheme)	Participants		Document	
	n	No. of references	*n*	No. of references
Security planning elements	8	132	10	52
Governance	8	88	6	13
Planning procedures	7	35	7	20
Security policies	3	9	9	19

Findings From Participant Interviews

Evidence from the data collection of the eight semistructured interviews and 10 institutional documents supports security planning as the second main theme followed by the subthemes of governance, security procedures, and security policies. Governance provides the structure and oversight for security planning, policies establish the fundamental principles and guidelines, and procedures detail the specific steps and actions needed to implement and enforce security measures. All three components work together to develop effective security strategies within the organization.

Governance. Governance in the context of security planning refers to the establishment of the framework, structure, and oversight mechanisms for security within an organization. This includes defining the roles and responsibilities of various stakeholders, such as the board of directors, executive management, and security teams. Effective security governance ensures that security is treated as a strategic priority, aligns with the organization's goals, and is appropriately funded and resourced. Table 6 illustrates the quantity of references pertaining to the subtopic of governance.

Table 6

References to Governance

Subtheme (secondary subtheme)	Participants		Document	
	n	No. of references	*n*	No. of references
Governance	8	88	6	13
Compliance	8	62	2	3
Risk planning	6	14	3	4
Insurance	6	9	1	4

Eight out of the eight interviewed participants referred to at least one governance-related element. P01 mentioned “So, we have been able to get money for the technical defenses that we think we need. I think there has been enough scary stuff in the news that our board and our other executives have been comfortable making those investments.” Regarding that same statement, P02 stated:

> The other component is the resourcing, depending on how well that case is made, or even if it has made very well, particularly in the last couple of years, capital markets have gotten very tough and so getting the money needed to deploy the people and or technology to be successful is becoming more difficult.

This quote presents the importance of establishing an organizational structure that can communicate so management can take the best-informed decisions regarding IS security. P03 directly mentions governance by stating “I have governance, risk and compliance”. P04 mentions the importance of audits when the participant said ”When you get an audit, the auditors are checking this stuff, and if you don't do it, the auditors will complain.”. On the same note, P05 stated “We do compliance, especially with ISO 27001, plus ISMS and ITIL.” Following that thought, P07 mentioned that the fourth or fifth step involves compliance, stating “You may have some breach obligations, instant reporting obligations.” The participant also stated, “So, I do think complexity and buy-in and governance is huge.” Working on regulation compliance is also an important factor for governance and P08 mentions “And then what I would add to that in terms of regulatory requirements, as a healthcare organization, the primary is HIPAA. PCI is another one that is important because they take credit card transactions.” Regulatory compliance is necessary because it aims to maintain cybersecurity industry standards while avoiding legal and financial repercussions.

Three subthemes emerged for the governance subtheme which include compliance, risk planning, and insurance as presented in Table 6. Eight out of eight participants referenced compliance as the first subtheme for governance. P01 mentioned “Five years ago, 10 years ago, people were worried about the HIPAA penalties and those costs. But honestly, those are nothing compared to the business interruption costs.” P01 mentioned “But these days I do not think the laws and regulations are nearly as impactful as the business aspect of this. It is the business interruption costs and the reputational

damage.” P03 stated “OCR [Office of Civil Rights] is the enforcement wing of that. But yeah, there is a ton of just regulation on reporting.” P04 mentioned “Now we are getting where we're at closer to 50 states having state laws of some way, shape or form. Then we have the SEC [U.S. Securities and Exchange Commission] coming forward saying you got to respond in 4 days, and you got OCR and the attorney general.” Following that same line of thought, P06 mentioned “The security exchange just put out their thing 4 days, respond to them. Attorney generals want you to respond. Office for Civil Rights wants you...everybody wants you to respond in X amount of time to an instant.” Healthcare regulation plays an important role in governance. P07 stated, “HIPAA is almost 30 years old. The security privacy rule upscale is about 20 years old.” The participant continued mentioning, “OCR is underfunded. They are a team of about 40, they can't deal with two or three healthcare organizations getting ransomware daily. So, healthcare regulation is very, very helpful. It at least gives you a benchmark.” P02 Commented on the lack of specificity stating, “Towards the effect of advanced adversary protections, the statutory requirements from HIPAA, even the auditable requirements from, say, Itrust, SoftTwo, or other frameworks, just flat out don't get the level specificity or completeness to go after modern advanced tactics.” The same participant continued stating, “And so, what we did as a system was break apart the tactic chain and come up with a set of requirements.”

Security frameworks are important in cybersecurity because they provide a comprehensive, organized, and adaptable approach to protecting an organization's digital assets. They help organizations reduce risks, achieve compliance, and continually

improve their security posture in an increasingly complex and evolving threat landscape. The participants mentioned different frameworks such as NIST, Zero Trust and PCI DSS. For example, P03 stated “Zero trust is super critical but it is also important to understand what makes up zero trust. That is a framework that is a mix of security and proper access and security management as well as monitoring.” The same participant stated “So, MITRE is a good framework to go through and make sure that you're looking at the top tactics that threat actors are using today, making sure that we then have those different log sources.” P05 mentions, “We do like it is a loose couple of integrations so that we are having only the data coming in a structured format…usually HL7 based. HL7 is health level 7 standard.” The participant continues stating, “That is predominantly for all the healthcare communications between two different organizations or two different systems.” P07 mentions as well, “We follow more of the seven based NIST 853 response mechanisms.”

Six out of eight participants referred to risk planning during the interview. Security risk planning plays an important role in protecting information systems. The importance of risk management is stated by P02 when expressing “yes, risk management is very tied to what we do in our information side.” P07 also expresses “So, we have a risk and compliance management program.” The most feared ransomware risks are third-party risk and zero day. P03 stated “Your tax service is expanding, but also having a remote workforce and then a lot of third parties. So, third-party risk. P06 validated this by commenting “Yeah, not that so much the organizations that I'm protecting, but what we're experiencing today is a lot of third-party issues.” That same participant stated, “The third

party is really the Achilles heel right now for us.” P04 mentions, “The worst attacks are zero-day attacks. If you get something that your security system has not seen before, you are the unlucky recipient of being the first one to get it, then you are in trouble.”

Transferring risk is important, therefore having insurance is important. Cyber insurance can help organizations manage the costs and challenges associated with cybersecurity incidents, including data breaches and cyberattacks. It provides financial protection and can help cover the expenses required for investigation, remediation, legal compliance, public relations, and potential liability claims. It also supports organizations in their efforts to enhance their cybersecurity posture and risk management practices. Six out of the eight participants mentioned insurance during their interview. P01 mentioned “Yeah, it would really stink to have to pay for credit protection for thousands of people. But honestly, we have insured for that risk.” P02 mentioned “Thou shalt have insurance for cyber.” as part of their cybersecurity commandments. P07 mentioned “And there's also aspects of it that I did not touch upon before on cyber-insurance, which is also an element of this as well. So, it is a key weapon in a multidimensional mature information security program.” Audits are linked to insurance. P04 mentions, “When you get an audit, the auditors are checking this stuff, and if you don't do it, the auditors will complain.” The participant continues stating, “If you try to get cybersecurity insurance, the insurance companies will complain and say, if you're not doing this, we're not going to give you insurance, or it's going to be a lot more expensive.” P04 finalizes the statement with the following sentence, “Insurance helps in those ways because it helps put the pressure.” On that same note P03 mentioned “Then I have my security analysts that are more like

analyzing, doing business process and audit remediations." This statement presents the need for organizations to be audited for cybersecurity and be able to correct audit findings as soon as possible. Remediation of audit findings is necessary for optimal protection of operations following industry regulations and standards.

Security Planning Procedures. Security procedures are detailed, step-by-step instructions that describe how specific security tasks and processes should be carried out. These procedures are part of the operational aspect of security planning. Table 7 illustrates the quantity of references pertaining to the topic of security planning procedures.

Table 7

References to Security Planning Procedures

Subtheme (secondary subtheme)	Participants		Document	
	n	No. of references	*n*	No. of References
Security planning procedures	7	35	7	18
Security plans	4	14	2	2
Incident response plan	4	9	5	10
Business continuity	3	12	5	6

On the security planning procedures, P06 mentioned "Cybersecurity strategy aligns in parallel with the business strategy." It covers various activities, including incident response, access control, data encryption, and more. To minimize risk, you need to have plans. P03 stated "So, I typically do a health check and then do a 1-, 3-, and 5-year plan. So, I align that to the business strategy and goals." The same participant mentioned "I need to do from more of a people and process is where we more aligned with the business to see what they're doing or their strategic plans."

Outsourcing of services is another topic discovered. Five out of eight participants mentioned the importance of outsourcing services. Outsourcing services require planning. For example, P03 stated “I have a big managed service partner because we know this day and age it's hard to keep and retain talent to really have those 24 by 7 operations.” This participant also stated, “So, that's where we go through with my managed service partners to make sure we have the technology capability, log sources, etc.” Following that same thinking, P06 stated “I think right now at a very high level, if an organization of any size is going to compete with the threat actors, then we're going to have to be more open to outside organizations helping us.” Still, P08 presents the issue of what happens if the outsourced organization is hit with a ransomware cyberattack when expressing, “When you outsource the management, which in a lot of cases is probably a good idea because that large organization that's protecting probably has more resources than you do.” The same participant continues stating, “But if they get hit, then what is your fallback? That becomes a challenge as well. It is not a fail-safe.” It is important to take into consideration all recommendations and weight options depending upon the organization’s needs. Partnering with other organizations has advantages that might help protect information systems from ransomware. P03 mentioned “We're an Epic Community Connect partner, so we're able to do a lot of stuff with our brick and mortar and putting our security practices on”. The same participant mentioned “And there have been a lot of good resources to help in this in healthcare, I think. H-ISAC [Health Information Sharing and Analysis Center] was great.” In the same vein, P07 stated, “And there have been a lot of good resources to help in this in healthcare, I think. H-ISAC was great.”

Four out of eight participants referred to incident response plans. P02 stated, “One requirement, thou shalt have incident response on retainer.” P03 follows the same thought expressing, “I have always focused on building the foundation of our tech stack to support systems from a protection monitoring alerting mitigation standpoint, but also having an incident response plan and retainer and all that ready to just in a moment's notice.”P05 reinforces this by mentioning “Then especially having a mediate response when something happens”. P07 follows up indicating “So, most organizations have a very robust ransomware response plan”. The same participant mentions “Over that, you'll have incident response and all of that you'll have ransomware playbook.” Premeditated steps and planned procedures help protect information systems from ransomware.

Three out of eight participants mentioned business continuity plans as the last subtheme for security planning procedures. P01 stated “So, with any of these things that you use to keep the bad guys out, you have to accept that a really determined bad guy will still get in. So, you have to have a business continuity plan.” P06 mentions, “What can I do to ensure its resilient and redundant? It is business continuity, DR, everything is there, and the security is in our layers to protect it, being isolated from the rest of the business where it can't be hit.” Part of the business continuity plan must involve having a data map. P08 mentions “And then having a data map. So where is the data? Which specific devices, which databases, which systems contain what data?” These questions need to be answered to know exactly where your position stands.

Security planning procedures are crucial for consistency and adherence to security practices. These security planning procedures create a proactive and comprehensive

approach to protect an organization's information systems. Continuous monitoring, adaptation to emerging threats, and regular review of security measures are essential for maintaining a strong security posture. Practicing protecting and recovering can be key to protecting information systems from ransomware cyberattacks. P01 follows that same line of thought when stating, “I think we can do better, as it is exactly what we were just talking about right now, which is the drills and the practice for how to recover.” Security planning involves testing current security plans while continually adjusting them to fit organizational security needs.

Security Policies. Security policies are high-level documents that outline the principles, guidelines, and rules for securing an organization's information assets. Security policies set the overarching framework within which security procedures and practices are developed and executed. They provide direction on what is acceptable and unacceptable in terms of security behavior and set the tone for security culture. Table 8 illustrates the quantity of references pertaining to the topic of security policies.

Table 8

References to Security Policies

Subtheme (secondary subtheme)	Participants		Document	
	n	No. of references	*n*	No. of references
Security policies	3	8	6	19
Cloud policies	2	2	2	2
Network policy	2	2	4	4
Data policy	1	1	2	2
Password policy	1	1	2	2
Incident response policy	1	1	2	3
Gartner’s risk and compliance policies	1	1	0	0

Three out of eight participants mentioned an aspect related to security policies. Cloud policies are important as cloud technology continues to be the selected solution. P05 states “Now, we are really looking to apply the best practices that Microsoft Azure had for healthcare organizations and following their best practices into our organization while mixing it with the policies that we have right now.” The cloud can play an important role in cybersecurity because as P07 stated, “Having an organization that can scale and respond appropriately that adopts the cloud in the right strategic part of your infrastructure”.

Examples of other policies mentioned during the data collection phase include when P01 mentioned that after an attack, “…we wound up with a 60-day password reset policy where everybody was forced to reset their passwords every 60 days.” Once data was restored in P01s organization, they were able to implement multi-factor authentication. P05 also mentioned the use of Gartner’s risk and compliance policies to create a playbook when stating “We have some resources that we took in place, especially from GRC, Gartner's risk and compliance. On one side, we were implementing those policies” This statement can be tied to the development and implementation of an incident response policy in order to react accordingly to a ransomware cyberattack, as P01 mentions:

> So, it [the incident response plan] informs from a policy and process perspective, helping us create the right playbooks so that our Security Cybersecurity Incident Response Team knows how they contain it and then how do they cleanse it out of our environment when something bad does get in.

Data policy was another policy mentioned as playing an important role to secure data as P05 mentioned, “Whenever they need data, we have our own data policy. Obviously, in that policy, IRB comes in place as well.” The participant continued mentioning “All the data that they were asking goes through the IRB and data stewardship, so that we make sure that it happens pretty much all through such as.” Also, P05 explains how security policies are spread among organizational levels by indicating “…we do place a comprehensive separate security policy and that policy really goes on to the top level, basically the strategic level and then on to the implementation level, then on to the operational level.” By aligning security policies with top-level management and securing their support and approval for security procedures, organizations can better protect themselves against cyber threats, demonstrate a commitment to cybersecurity, and reduce the likelihood and impact of security incidents.

Effective security policies are essential for protecting information systems from ransomware attacks. Security policies provide a framework for organizations to establish a proactive and holistic approach to ransomware prevention and response. They guide the implementation of technical and procedural measures that, when properly followed, can significantly reduce the likelihood of a successful ransomware attack, and minimize the impact if an attack occurs.

Findings From Industry Documents

Ten industry documents were collected and examined to observe how they support the security planning theme, as well as its’ subthemes which include governance, security planning, and security policies. For example, ID01 presents the importance of

developing and implementing an incident response plan, particularly a ransomware response plan. This industry document also reaffirms the importance of having cyber insurance in place in case any ransomware attack affects patient's health data. The content of ID01 also identifies the importance of establishing security policies around ransomware, such as phishing policy and an organization-wide policy regarding ransomware attacks. ID02 also checks the importance of having an incident response plan as well as include as password policy to change all system passwords once a ransomware attack has been contained. ID03 confirmed information regarding risk planning and the importance of engaging with information sharing and analysis centers, information sharing and analysis organizations, and CISA to be informed of posing threats. In that same line of thought, ID08 recommends establishing relationships with third-party cybersecurity service providers and using their expertise to assist in improving their protection against ransomware. ID03 also supports the idea of security planning to define an HCO's cybersecurity capabilities and then act upon them. The content of ID04 confirms the importance of clear communications between leadership and employees to accurately establish executive support towards security issues. ID05 validates business continuity planning as an important element towards ransomware response. ID06 ratifies how network policy such as using a modern and secure browser can help prevent ransomware attacks, as well as how cloud vendors include built in ransomware detection and recovery. ID07 establishes the importance of stakeholder contribution to improvements in security planning and execution. ID07 also validates the use of security policies, particularly when disposing of hardware that had critical data, so it does not fall

into the wrong hands for phishing use. ID08 also supports security policies as important strategies to prevent ransomware attacks. The content of ID09 indicates to use network security policies such as network segmentation by business areas to minimize damage in case of a ransomware cyberattack. ID10 further presents the importance of using trusted channels whenever reporting a ransomware incident to law enforcement in order to protect vendors and customers and follow compliance. All 10 documents support the study's findings on how governance, planning procedures and policies interrelate while building an effective security planning foundation.

Connections to Effective Information Security Practices Found in the Literature

The findings of this study evidence how information security planning aligns with existing literature. It is important to strategize information security planning in the organization before developing and implementing information security policies and the SETA program (Alghazo et al., 2023). As presented by the eight study participants, information planning elements play a pivotal role in the protection of information systems from ransomware. Fisher et al. (2021) noted the need for readiness and vigilance to minimize cyberattack-related disruptions. The importance of organizational areas defining trusted communication channels to help strategize security plans such as incident response and business continuity plans is important to mention. These plans are vital for preempting, handling, and recuperating from cybersecurity occurrences. P06 mentioned "cybersecurity strategy aligns in parallel with the business strategy." This means that these plans do not only facilitate proficient reactions to security breaches but also guarantee the enduring steadiness of operations and robustness of the enterprise,

even when confronted with disruptive events like a ransomware cyberattack. Fisher et al. (2021) insists that ensuring appropriate plans and procedures are in place to respond and recover from an attack are critical to maintaining operations of information system assets.

According to Ahmad et al. (2021) the three key areas of organizational security as defined by the joint task force on cybersecurity education are risk management, planning and strategy, and policy and governance. These same security elements were identified as some of the most important subthemes for the security planning element's theme under the governance subtheme in the data analysis results of this research. Governance ensures a balanced consideration of stakeholders' requirements, circumstances, and choices (Savaş & Karataş, 2022). This act of balance ensures cybersecurity. It simplifies the evaluation of management and leadership in decision-making and setting priorities, as well as an assessment of shared institutional objectives (Savaş & Karataş, 2022).

Security planning procedures include response planning. Response planning refers to the planning stages of maintenance of processes and procedures to ensure the response to a detected cybersecurity incident (Sulistyowati et al., 2020). Incident response plan and business continuity are important strategies to have in place. Having an incident response policy in place helps define the steps to take when a ransomware attack is suspected, including isolating infected systems, and notifying relevant authorities. The business continuity plan presents how security procedures support operations resiliency.

Information security policies are a set of documented guidelines, rules, and procedures that organizations develop and implement to protect their information assets and data from various security threats and risks. Information security policies within an

organization should be the basis for all information security plans (Nord et al., 2020). These policies serve as a foundation for establishing a secure network while ensuring the confidentiality, integrity, and availability of information. If the organization has a failure in planning and implementing policies for cyber security, then that will incur vulnerabilities in the system (Upadhyay & Sampalli, 2020).

Connections to the Conceptual Model and Other Studies

Evidence collected from the interviewed research participants as well as existing literature confirms the theme of information security planning as an important strategy to protect information systems against ransomware cyberattacks. When viewing the information security planning theme through the GST lens, HCO IT leaders that implement and test information security plans will holistically contribute to increasing the overall information security health of the organization. Overall, governance, planning procedures, and policies are interrelated components that form the foundation of effective security planning. In the concept of governance, not only governments or institutions have roles, but also individuals and the private sector (Savaş & Karataş, 2022). Governance sets the strategic direction and accountability, planning procedures outline the steps to achieve security goals, and policies provide the specific rules and guidelines to implement and enforce security measures. Together, they create a holistic approach to information security planning. Four out of eight study participants viewed ransomware protection as an organizational issue not just an IT problem. Consistent with von Bertalanffy (1968), in GST, the individual elements of the system work together as a whole to achieve the central objective. Abraham et al. (2019) mentions that healthcare

organizations have a responsibility to leave no stone unturned by taking a proactive and holistic approach to cybersecurity preparedness. This same line of thought confirms that information security planning plays a fundamental part in information security ransomware protection strategies.

Theme 3: Human Security Elements

Human security elements was the third significant theme to arise from the data analysis phase of this study. Human factors are a pivotal component of information security, but assuming that individuals will consistently adhere to secure behavior patterns and meet information security expectations is not always a valid assumption (Hughes-Lartey et al., 2021). Despite this level of understanding, organizations continue to focus their attention on technical security controls rather than human factors (Evans et al., 2019). Irrespective of the implementation of different technical solutions, human elements remain an aspect that often receives insufficient consideration (Hughes-Lartey et al., 2021). Organizations continue to suffer information security incidents and breaches as a result of human error even though humans are recognized as the weakest link with regard to information security (Evans et al., 2019). Acknowledging the importance of human elements in information security is imperative, and organizations must prioritize addressing human factors alongside technical security controls to effectively mitigate the risks associated with human error and enhance overall information security resilience. The human element theme for this study is divided into the following subthemes: security training, and security awareness. Table 9 illustrates the quantity of references pertaining to the topic of human security elements.

Table 9

References to Human Security Elements

Major theme (subtheme)	Participants		Document	
	n	No. of references	*n*	No. of references
Human security elements	8	75	7	15
Security training	7	41	5	8
Security awareness	7	33	6	7

Findings From Participant Interviews

Evidence from the data collection of the eight semistructured interviews and 10 industry documents support human security elements as the third main theme followed by the subthemes of security training and security awareness. Security training and awareness are interconnected elements of a holistic approach because training provides the knowledge and skills, while awareness ensures that individuals maintain a vigilant and proactive stance in safeguarding against security threats. Both components work together contributing to building a resilient and security-aware organizational environment.

Security Training. Security training involves the process of educating individuals within an organization on various aspects of security, with the aim of enhancing their knowledge, skills, and awareness to effectively mitigate security risks. The primary goal of security training is to equip individuals with the necessary information and capabilities to protect the organization's information, assets, and infrastructure from potential threats, breaches, or unauthorized access. Cybersecurity education is an essential factor to consider when addressing ransomware as it is a

proactive and preventive measure that empowers individuals and organizations to protect information systems. Table 10 illustrates the quantity of references pertaining to the subtopic of security training.

Table 10

References to Security Training

Subtheme (secondary subtheme)	Participants		Document	
	n	No. of references	*n*	No. of references
Security training	7	41	5	8
Security training program	7	34	5	8
Training as a black hole	2	2	0	0
Training is somewhat effective	2	2	0	0
Track trainings	1	2	0	0

Seven out of the eight interviewed participants referred to at least four security training elements. P01 mentioned "So, we do training every year as part of our compliance training. We make sure that everybody understands what their responsibility is." The same participant followed up with the following comment "We also do tests, so we do phishing tests to see if people are going to click links or open attachments." P02 stated "From a strategy perspective, having a well-trained and thoughtful security team is important. The same participant mentioned "Regular phishing exercises…when I say regular it's at least monthly." P03 establishes the importance of allocating budget to training by mentioning "Budget is always an issue that everyone is fighting for dollars in healthcare, but training is really a low-cost no-cost. We do tailored training based off of people's roles. Higher risk users get more defined training with examples." P04 mentions the importance of tracking training by stating that "…what you should do is most places

are required to have regular training. So usually, you give training every 6 months or something like that, where you give people training just in general on cybersecurity and safety." Having consequences is important if training is not followed as P04 states, "Send them reminders, if they haven't done it, it'll escalate to their supervisor, if they haven't done it, it'll send it an audit trail if these people took the training or didn't take the training." The participant continued on mentioning, "You can decide what happens if they do not do the training within a certain date. You can keep sending reminders, or you could do something else to escalate it." P04 also mentions the phishing tests as "Then there is the testing piece of it. And they recommend that you do some kind of testing like once a month". P05 also commented on prioritizing on team training "…we have a team that's trained on cybersecurity because this was the priority for us." P06 validates how education involves phishing tests when stating "We had talked about education, which includes phishing simulations." On that same note, P08 communicates that:

> Most organizations, mine included, do things like simulated phishing attacks. In that instance, we will send what appears to be a phishing email out to the broad population, and we will track how many or what percentage of people respond, which how many click on it, how many open attachment or how many give away credentials, how many of those that click on it, of course, then are assigned training, and then we track those that have completed the training, we try to make them required.

All participants that mentioned using phishing exercises used the software KnowB4 as a solution. P04 mentions exactly "There's a vendor that I've used that's very good, where

they allow you to do testing, where you send out a fake cyberattack, and like a phishing test…the product that I've used the most is something called KnowBe4."

Establishing a security training program is important to all system users. Seven out of eight participants talked about their established security program. One of the main elements of the program involves identifying a security team and training them. Six out of eight participants mentioned the need to have an experienced security team, as well as a qualified incident response team to do the work and receive training in their areas to continue skilling up against ransomware threats. P08 stated "As people get more and more skilled up, having them take on more and more of the deeper technology challenges." On that same line of thought P01 mentions on training that it "highlights the importance of being ready to respond when there's a successful attack." Training is an important piece to the information security puzzle against ransomware. P07 mentions that "you do have to compensate with things like rapid response or accepting a level of resilience." This is exactly where training plays an important role. For example, as P01 also mentioned, "The folks at the service desk have to recognize the difference between something that's clearly user error or a common technical glitch, versus something more serious, an event and we have them escalate to the Security Incident Response Team." Knowing what each team member needs to do before, during, and after an incident helps maintain order, logic, and structure during a ransomware crisis, and this can be achieved with training. Training is effective when employees use the knowledge for the organization's benefit. Because training takes time, money, and resources it can be seen as a tracking investment. Due to the lack of cybersecurity skilled personnel in the

industry, it is difficult to find and retain IT employees overall, affecting the training plans. P07 expressed his concern on the staff topic stating, “Did I mention that the talent marketplace right now is on fire, right?” meaning that there has been a lot of turn-over in cybersecurity positions. P03 confirms this when mentioning “I have a big managed service partner because we know this day and age it's hard to keep and retain talent to really have those 24 by 7 operations.”

Two out of the eight participants do not fully support training as a form of protection, mentioning directly that can be somewhat ineffective. P08 mentioned that “training or security awareness will be somewhat effective.” Following the same line of thought P02 stated “But with the training, we just have to assume there is one sucker in every crowd. So, if you are relying on your training to prevent a threat, it is not a very successful strategy, not a very advisable strategy.” P03 warns us on the importance of effectiveness of training employees by stating “Also make sure that you get creative in your messaging, training, and awareness because you can spend millions of dollars on security.” The participant continued “It's a deep dark hole on that if you're not training and communicating with your end users, you're never going to be successful.” Training effectiveness and human behavior are questioned by P04 when the participant mentions:

> So, I used to joke about one of the things I found after a couple of trainings, as people usually start to get good at cybersecurity, behaving and doing the right thing. So, you send them these Citibank things and Bank of America and they completely ignore them. But if you send them one email link looking like a

coupon for free Dunkin Donuts or free Starbucks coffee, immediately they forget everything learned, and click on it.

Security Awareness. Security awareness in cybersecurity refers to the knowledge and understanding that individuals within an organization have about the importance of cybersecurity, the potential risks and threats to information systems, and the best practices for protecting sensitive data. Table 11 illustrates the quantity of references pertaining to the topic of security planning procedures.

Table 11

References to Security Awareness

Subtheme (secondary subtheme)	Participants		Document	
	n	No. of references	*n*	No. of references
Security awareness	7	33	7	7
Employee security awareness	6	22	1	1
Awareness training	4	11	1	1

***Employee Security Awareness*.** On employee security awareness, six out of eight participants mentioned at least two references for employee security awareness. For example, P04 mentioned "…no matter what you do, if you don't do user education, you made a mistake." Meaning it takes an educated team to create a security culture where learning is key to protection. P01 stated on the interview "Ransomware attacks help us have conversations with people in operations, the non-IT people, so that they understand as good as we like even if we're close to perfect, it can still happen." Following that same of thought on security awareness, P04 also stated "One strategy which overall, no matter what you do is the most important, it's education." The same participant continued

mentioning “It's really important to teach users about being careful, about clicking links and emails, and putting USB drives into computers, and things like that. Just being cautious and careful about what they do.” Following on the same topic, P05 mentioned “The first thing is training the people, by giving them the awareness.” making security awareness a basic strategy to consider when protecting information systems from ransomware attacks. It is important to have communication gateways that create threat awareness upon users, as stated by P05 when mentioning “We dish out some messages to the entire network of the users through emails and through the other communication gateways that we have so that they are aware that these threats are there.” Awareness has also impacted the executive level and buy-in investment for the better, as P08 recounted, “Since ransomware, the last several years, has been prevalent in the news cycle, it's given cybersecurity a lot more attention. That is at the board level, that's at the executive level.” The participant continued stating “So it used to be years ago, you used to try to talk about information security and it would fall in deaf ears.” The same participant mentioned that because of the awareness, investment in cybersecurity has occurred, particularly when mentioning, “…making people understand the importance, gaining mind share, getting dollars to invest in the program, and continually reporting on successes of what the team has been able to accomplish based on the investment.” P06 validates this thought when stating, “Now, it has the awareness around it, and it has the financial bind to it as well.”

National security requires keeping critical infrastructure protected against ransomware threats. It is worth mentioning a comment made by P06 on cyberwarfare stating, “If we went into cyberwarfare and these ransomware attacks never happened, we

wouldn't be as prepared as we are." The participant continued "But still we have a long way to go so U.S. healthcare infrastructure in order to withstand cyberwarfare." P06 goes on mentioning "I am a firm believer that if it wasn't for these people doing what they're doing, and I don't condone it... In the event of a cyberwarfare perspective, we would not prevail very well." According to the participant's statement, HCOs in the United States are not prepared to protect IS in case of a cyberwarfare event.

Awareness Training. Four out of eight participants mentioned some sort of comment regarding awareness training. P06 mentioned, "I don't feel you can be successful without the opportunity or ability to communicate to your peers, to the organization, and shift the culture inch by inch by inch to be aware." Following that same line of thought, P07 stated "…you're continually educating, you're sending out new vectors to your threat team, to your audience, your community, so that they're aware of the latest attack factors." These words validate that not only individual system users are part of the awareness training, but top management is also impacted on awareness as well. For example, P01 mentioned, "Awareness starts at the top and then there's the annual training that gets it to everybody, but then the drills…We did a tabletop exercise a couple of weeks ago…" The participant continued mentioning "We pulled people from Corporate Communications, from Legal, from treasury. We wanted to make sure that we had a broader group of people that had the ability to respond in a crisis appropriately if we have been attacked." P07 states that they create awareness training using "…whether it's tabletops or pen tests or external strategic assessments." The same participant also mentioned that "Most organizations have a very robust ransomware response plan and

also exercise, going through penetration tests and tabletop exercises, including the senior executives." Aligning the visions of all employees and levels along with the organization's cybersecurity culture always depends on budget allocation and senior buy-ins. For example, P02 stated "Well, the good news is that cybersecurity was seen as hard and fast requirements, which made commanding the required funding to support it easier, which helped." The same participant continued mentioning "And we got buy-in all the way up to the senior Echelons, think C-suite as the fees were needed and tied it to risk."

There is no doubt that the human element plays an important role when protecting IS against ransomware attacks. Awareness training is crucial when protecting against ransomware because human error is often a significant factor in the success of ransomware attacks. Ransomware typically involves tricking users into clicking on malicious links or opening infected attachments, which then allows the ransomware to infiltrate the system. P06 validates this when the participant mentioned "When you think about people side of things, awareness has been key." Awareness training is an integral part of a comprehensive cybersecurity strategy, as it empowers individuals within an organization to recognize, resist, and report potential ransomware threats. Education and awareness training strategies can significantly reduce the risk of ransomware cyberattacks.

Findings From Industry Documents

Ten industry documents were collected and examined to observe how they back the human security element theme, including its' subthemes which include security training and security awareness. For example, ID01 presents the significance of

incorporating and rigorously administering regular phishing training to reduce human errors and mitigate potential system vulnerabilities. This industry document also reaffirms the use of ransomware security incidents as knowledge gaining experiences that emphasizes the need for phishing and cybersecurity awareness. ID02 mentions the importance of cybersecurity training using compulsory cybersecurity awareness trainings to keep users aware of the most recent cybersecurity threats and practices. ID03 presents the idea of planning and implementing a SETA program that includes awareness for the users on the need of identifying and reporting suspicious incidents, for example phishing activity. ID04 presents phishing attack testing campaigns as a solution towards employee security awareness. ID05 mentions the lack of ransomware training for staff in organizations as ransomware attacks keep rising. ID07 mentions the importance of staff training at every level, including IT, to eliminate insecure system configurations and unsafe practices. ID10 talks about training and awareness through software hygiene, social engineering awareness and training exercises. Seven of the 10 industry documents support the study's findings on how human elements such as training and awareness cybersecurity strategies help protect IS from ransomware cyberattacks.

Connections to Effective Information Security Practices Found in the Literature

The findings of this study evidence how human elements in information security training and security awareness line up with existing literature on protection strategies against ransomware attacks. The literature evidences the theme of human security elements as an important strategy to protect HIS against ransomware. The subthemes of employee security awareness as well as awareness training also align in support with

existing literature. The accumulation of information security knowledge by employees over their lifetimes and through participation in awareness, training, and education initiatives positively contributes to the cultivation of an organizational information security culture. (Da Veiga et al., 2020). The subtheme of security training is also linked to user training, as it helps eradicate change resistance, while driving closer inspection on users (Sandar et al., 2019). But security training is also linked to management training. Senior management should undergo training to acquaint themselves with system users, fostering a heightened awareness of user-specific access privileges and internal channels that could potentially grant access to confidential information (Sandar et al., 2019). According to Da Veiga et al. (2020), SETA programs are the resolution to creating a good security culture. A critical measure to increase cybersecurity involves establishing awareness training programs for users and employees (Alkhazi et al., 2022).

Connections to the Conceptual Model and Other Studies

Evidence collected from the research participants and existing literature confirm the theme of human security elements as a main strategy to protect HCOs' IS against ransomware cyberattacks. This theme is in alignment with GST, which is the conceptual framework of the research. When viewing the human security theme through the GST lens, there is a need to look at the whole while analyzing single elements and concentrating on their associations and relationships (Battistoni et al., 2019). Consistent with von Bertalanffy (1968) GST presents the individual elements of the system working collectedly as one entity to achieve a central objective. Holism is considered an underlying principle of GST (Wymer et al., 2023). The recognition of the

interdependence among individual components within a system and between the system and its environment allows for the delineation of the system's boundaries, thereby establishing an identity devoid of isolations (Battistoni et al., 2019).

The realm of cybersecurity is profoundly shaped by the impact of training and awareness on human behavior. The provision of security awareness training courses holds the potential to comprehensively influence attitudes toward the management of information security (Zwilling et al., 2022). Cybersecurity training programs aim to educate individuals about the risks, best practices, and measures they can take to protect themselves and their organizations from threats such as ransomware. Creating a culture of cybersecurity awareness within an organization is crucial for building a collective commitment to security practices. An organization's information security culture guides the organizational activities related to the protection of IS while influencing stakeholder's perception and behavior positively on cybersecurity (Da Veiga et al., 2020).

Application to Professional Practice

Security management practices was the first major theme to be revealed using thematic analysis. Security management practices pertains to technical defense practices as well as protective technology tools and solutions. Security planning elements was the second main theme to arise from the thematic analysis, pertaining to governance, security planning procedures and security policies. The third and final discovered theme was human elements pertaining to security awareness and security training. The protection of IS is a shared responsibility between management and users. Management should plan and enforce the necessary security controls and policies while also considering

information security budget decisions to buy security tools that align with proper cybersecurity measures, fomenting employee training towards stronger digital hygiene (Argaw et al., 2020), increasing user awareness.

Based on evidence from the research's findings it is important for HCO leadership to employ and retain knowledgeable and experienced IT leaders, when overseeing technical perspectives and managerial approaches towards ransomware protection and cybersecurity. Information security management is the process of applying security practices and controls to protect information assets in an organization (Topa & Karyda, 2019). At the same time, the second theme is tied to the first theme of security management as security planning is needed to effectively strategize the use of security procedures and protective systems. Strategizing information security involves the implementation of information security policies and procedures in compliance with governance. Information security policy, procedures and standards should align with best practices to help establish shared values and beliefs among system users (Da Veiga et al., 2020). Planning plays a crucial role for management in maintaining policy, procedures and governance aligned from a cybersecurity perspective. The second theme is tied to the third theme as human elements shape positive cybersecurity behaviors with SETA training to all level employees to create more security awareness (Topa & Karyda, 2019). At the same time, the development of a cybersecurity training program to the IT staff on cybersecurity technical procedures and response is needed to increase cybersecurity awareness, thereby increasing protection of HCO information systems from ransomware cyberattacks. Organizations should help individual employees protect against

ransomware (Chung, 2019). Problems or challenges related to personnel, particularly in the context of security, can be successfully resolved by implementing security training and awareness programs. These programs are designed to enhance the knowledge, skills, and awareness of individuals within an organization regarding security practices and protocols. If a company's security initiative fails to enable employees to safeguard themselves, there is a higher likelihood that they will take actions jeopardizing the network's security (Chung, 2019).

The findings from this research can act as a valuable information asset to HCO IT leaders in identifying important security management strategies practiced while using technical defense and protective technology tools and solutions. Organizations need to be equipped with advanced technical solutions to deal with cybersecurity threats (Singh & Gupta, 2019). The use of technical equipment aligned with the right management practices can help protect IS from ransomware cyberattacks. Research findings present recent security management practices such as identity management, network management, vulnerability management, and technical control testing can help information security leaders to protect IS from ransomware cyberattacks.

Also, the research outcomes may act as an information resource that links security management practices to security planning elements such as governance, policies, and procedures. Strategizing and organizing different security plans are necessary from a security management perspective when protecting IS from ransomware. In the absence of established protocols, the necessity for timely security updates, and the government's emphasis on maintaining the security of devices and applications, organizations may face

formidable security challenges (Newaz et al., 2021) without proper security plans. Leveraging the results of this study can support the development of a security planning and design strategy that considers current ransomware trends and security threats.

Other findings of this study may serve as information resource for upcoming healthcare security training and awareness to IT leaders. While security management and planning of technical defense mechanisms hold significant importance, individual behavior and adopting a positive 'online lifestyle' are equally crucial (Connolly & Wall, 2019). A singular technological solution is insufficient to eradicate the ransomware threat. Therefore, a comprehensive strategy is necessary, encompassing socio-technical measures, vigilant front-line managers, and active support from senior management (Connolly & Wall, 2019). Security training and awareness play a crucial role in the protection of IS from ransomware cyberattacks, therefore education and awareness to for all employees including c-level management and the cybersecurity team has to be taken into consideration when protecting HCOs from ransomware cyberattacks.

Implications for Social Change

The findings of this research may help save HCO IT leaders from the ordeal and chaos related to a ransomware cyberattack. Ransomware attacks present a risk not only to the identity and financial well-being of patients, but also to HCO operations as they have the potential to disrupt hospital operations, jeopardizing the health and safety of patients (Argaw et al., 2020). Ransomware cyberattacks may disrupt day-to-day operations including patient care, appointments scheduling and billing. Recovering from a ransomware attack can be a lengthy process as HCO IT leaders may need to rebuild

systems, restore data from backups, and conduct thorough cybersecurity assessments to prevent future incidents. This downtime can have lasting effects on patient care and overall HCO operations. Considering that health systems demonstrating high achievement have the potential to enhance community health (Thamer & Alubady, 2021), it is imperative for IT leaders of HCOs to keep focus on cybersecurity strategies and trends to protect IS from ransomware. The findings of this research may contribute to society by ensuring patients health data is secure, while helping them receive the needed care towards a better life without interruptions.

Recommendations for Action

The strategies that emerged from the semistructured interviews conducted with eight participants and 10 industry documents can be valuable in assisting other IT and security leaders globally regarding the adoption of protection strategies against ransomware attacks. Utilizing the findings from this research, I developed beneficial recommendations that can be used and implemented to successfully protect information systems from ransomware cyberattacks. IT leaders and managers can use the following recommendations to protect information systems from ransomware cyberattacks. In light of the research outcomes, I propose the implementation of the following measures and actions.

As a primary recommendation, IT and security leaders should assess, review, and compare existing security management practices for protecting IS from ransomware attacks. The assessment will help identify which technical defense practices are aligned with different protective technology tools available in the market. The implementation of

security controls such as identity management, network management, vulnerability management and technical control testing are considered necessary technical defense practices when protecting information systems from ransomware attacks. Email protection, endpoint protection, AI, backup protection, and antivirus software are crucial security management tools that should be integrated with technical defense practices to help protect information systems from ransomware.

The second recommendation pertains to the necessity for security leaders to evaluate their security planning components, with a focus on governance, planning procedures, and security policies, to ascertain their alignment with the findings of this study. IT leaders should strategize protection of IS from ransomware, while taking into consideration the newest ransomware cyberattack trends. Security governance should be treated with strategic priority aligning with organizational goals, risk plans, and security resources. Risk planning and cyber insurance are necessary elements that help with ransomware risk. Developing, implementing, and testing plans particularly, business security, incident response, and business continuity plans must be part of the security planning procedures. IT leaders need to identify and follow a security framework such as NIST or MITRE, providing proven guidelines to follow when protecting information systems from ransomware. Reviewing security policies will set the overarching framework to align with security best practices and procedures to make sure they get executed organizationally. HCO IT departments searching for planning elements and strategies to protect from ransomware cyberattacks should examine this study findings to learn if the strategies are viable in their organization.

The third and final recommendation relays the need for HCO IT leaders to assess human security elements for employees such as security training, as well as security awareness. Training programs impart knowledge and skills, while awareness training ensures individuals adopt a vigilant approach to ransomware protection as both elements collaborate to establish a resilient and security-conscious organizational environment. Training plans should be tracked and monitored per user to help create better security awareness by influencing security behavior in users. IT leaders need to establish a security awareness plan that affects top management, IT employees, and all users. Creating an effective cybersecurity culture requires education and training strategies, as impacted behaviors can better protect information systems from ransomware attacks. Research findings reassure ransomware training and awareness as the third main strategy to protect HCO IS from ransomware attacks. HCO IT leaders should take into consideration the three mentioned recommendations, so they adopt a solid IS security stance to protect against HIS from ransomware attacks.

I will use various methods to share this study's results. Once the capstone is approved by Walden University's chief academic officer, a summary of the findings will be shared with all participants. The capstone document will also be published in the ProQuest Dissertations & Theses database, a vast repository housing dissertations and theses, academic journals, and reports. Additionally, I intend to publish the research in various scholarly journals, reports, conferences, and other academic publications to enhance its visibility and reach other IT & security professionals.

Recommendations for Further Research

This study revealed some of the strategies IT and security leaders use in HCOs to protect IS from ransomware cyberattacks. The focus of this study involved identifying ransomware protection strategies HCO IT leaders from the United States use to protect IS from ransomware attacks. The first limitation for the study involved interviewing only IT leaders from HCOs in the United States. The research's sample will represent the studied population to transfer its findings to U.S. HCO IT leaders. Broadening the scope of the study to encompass other country HCOs would serve to authenticate participants' perspectives and ascertain the applicability of identical outcomes in the sector, validating its broad applicability. It is suggested that this research be replicated in HCOs of other countries as well.

The second limitation for this research involved obtaining the study's sample size to provide sufficient data to answer the central research question. Data saturation was used to determine when there was enough research data to build a solid comprehension of the research phenomenon. I ceased data collection after eight interviews, when I found redundancy within the same findings of all participants. Triangulation provided data when cross-referencing interview data with member checking sessions, and then comparing themes with industry documents. A quantitative research design can help a researcher obtain more participants in the data collection process, increasing sample size. It is recommended to evaluate the main research question using another research design to study the similar research objective to compare results.

The third limitation involved the variation of participants' experience levels. The study was limited to inviting IT leader participants who have worked as chief information officer or chief information security officer for HCOs in the United States for more than 5 years of experience and that had applied cybersecurity strategies in HCOs to protect IS from ransomware cyberattacks. Involving participants with HCO IT job descriptions other than chief information officer or chief information security officer, such as chief technology officers or IT vice presidents, who are also involved in cybersecurity strategy implementation, and can contribute to identifying strategies to protect information systems from ransomware cyberattacks.

Reflections

In my quest to explore the strategies IT leaders from HCOs use to protect information systems from ransomware cyberattacks, through my coursework and research, I observed the complex nature of the ransomware threat in the healthcare environment, tied to current existing strategies that protect IS from these threats. The coursework prepared me to adopt fine research skills as well as gaining knowledge in cybersecurity subject matter. This research has been my most challenging academic endeavor ever, but I feel it was for the best. Determination, persistence, organization, and patience have been critical factors that helped me surpass this lifechanging journey. Balancing time between personal, family, and work-related responsibilities was a difficult task that led me to realize that you can never have full control of life, therefore, you need to establish priorities and mesh them with to-do lists.

This academic opportunity gave me the chance to establish a bond with my peers and subject matter experts in information security knowledge and research skills as well. I was able to brush up on my reading, analyzing, and interpretation skills also. My writing skills also improved when working throughout class assignments, reports, discussions, and doctoral research. This study has widened my perspective on the information security topic, while also gaining research experience when working with academic research standards. I have the utmost admiration for doctoral students and doctors, as they generate knowledge in their fields following difficult work.

To enhance the credibility of this study I employed the use of research methodology to eliminate personal bias from influencing the research track. I also adhered strictly to an interview protocol that was used uniformly with all study participants, providing them with the opportunity to calendarize member checking sessions to verify the authenticity of the recollected information. Following the interview protocol as a guide, I adhered to the doctoral study ethical guidelines to produce authentic results.

The pandemic made me reanalyze the study design and process, maybe for the best. An example of a change included collecting the data using a synchronic videoconference platform to interview the study participants. My previous career and technological experiences helped me complete the videoconference interviews in a professional manner. Participants were understanding of this situation and collaborated with their answers willingly, helping generate insights on the strategies HCO IT leaders use to protect information systems from ransomware cyberattacks.

Conclusion

Information technology leaders and management should revise existing security programs and strategies, focusing on security management practices and protective technology use tools. The incorporation of robust security policies and procedures along with reshaping user activities with skillful planning, training and awareness aimed at managing ransomware threats play a crucial role in significantly reducing ransomware attacks within information systems in HCOs. The findings from this study included three strategies that IT leaders use to protect information systems from ransomware attacks in HCO's; (a) implement and align technical defense practices with protective technology tools, (b) assess and align security planning elements such as governance, procedures, and policies, (c) monitor and measure human security elements such as security training and security awareness.

References

Abdullahi Yari, I., Dehling, T., Kluge, F., Geck, J., Sunyaev, A., & Eskofier, B. (2021). Security engineering of patient-centered healthcare information systems in peer-to-peer environments: Systematic review. *Journal of Medical Internet Research*, *23*(11), Article e24460. https://doi.org/10.2196/24460

Abraham, C., Chatterjee, D., & Sims, R. R. (2019). Muddling through cybersecurity: Insights from the U.S. healthcare industry. *Business Horizons*, *62*(4), 539–548. https://doi.org/10.1016/j.bushor.2019.03.010

Abu-Amara, F., Almansoori, R., Alharbi, S., Alharbi, M., & Alshehhi, A. (2021). A novel SETA-based gamification framework to raise cybersecurity awareness. *International Journal of Information Technology*, *13*(6), 2371–2380. https://doi.org/10.1007/s41870-021-00760-5

Addeo, F., Delli Paoli, A., Esposito, M., & Ylenia Bolcato, M. (2019). Doing social research on online communities: The benefits of netnography. *Athens Journal of Social Sciences*, *7*(1), 9–38. https://doi.org/10.30958/ajss.7-1-1

Adkoli, B. V., & Parija, S. C. (2019). Systems approach in medical education: The thesis, antithesis, and synthesis. *Tropical Parasitology*, *9*(1), 3–6. https://journals.lww.com/tpar/fulltext/2019/09010/systems_approach_in_medical_education__the_thesis,.2.aspx

Ahmad, A., Maynard, S. B., Motahhir, S., & Anderson, A. (2021). Case-based learning in the management practice of information security: an innovative pedagogical

instrument. *Personal and Ubiquitous Computing*, *25*, 853–877. https://doi.org/10.1007/s00779-021-01561-0

Alghazo, S. H. A., Humaidi, N., & Noranee, S. (2023). Assessing information security competencies of firm leaders towards improving procedural information security countermeasure: Awareness and cybersecurity protective behavior. *Information Management and Business Review*, *15*(1[I], Suppl. I), 1–13. https://doi.org/10.22610/imbr.v15i1(i)si.3408

Alkhazi, B., Alshaikh, M., Alkhezi, S., & Labbaci, H. (2022). Assessment of the impact of information security awareness training methods on knowledge, attitude, and behavior. *IEEE Access*, *10*, 132132–132143. https://doi.org/10.1109/ACCESS.2022.3230286

Alshaikh, H., Ramadan, N., & Hefny, H. A. (2020). Ransomware prevention and mitigation techniques. *International Journal of Computer Applications, 177*(40), 31–39. https://doi.org/10.5120/ijca2020919899

Andrzejewski, K. (2019). Security information management systems. *Nauki o Zarządzaniu*, *24*(4), 1–9. https://doi.org/10.15611/ms.2019.4.01

Antonio, M. G., Schick-Makaroff, K., Doiron, J. M., Sheilds, L., White, L., & Molzahn, A. (2020). Qualitative data management and analysis within a data repository. *Western Journal of Nursing Research*, *42*(8), 640–648. https://doi.org/10.1177/0193945919881706

Argaw, S. T., Troncoso-Pastoriza, J. R., Lacey, D., Florin, M.-V., Calcavecchia, F., Anderson, D., Burleson, W., Vogel, J.-M., O'Leary, C., Eshaya-Chauvin, B., &

Flahault, A. (2020). Cybersecurity of hospitals: Discussing the challenges and working towards mitigating the risks. *BMC Medical Informatics and Decision Making*, *20*, Article 146. https://doi.org/10.1186/s12911-020-01161-7

Armstrong, S. C., Lensen, S., Vaughan, E., Wainwright, E., Peate, M., Balen, A. H., Farquhar, C. M., & Pacey, A. (2021). VALUE study: a protocol for a qualitative semi-structured interview study of IVF add-ons use by patients, clinicians and embryologists in the UK and Australia. *BMJ Open*, *11*(5), Article e047307. https://doi.org/10.1136/bmjopen-2020-047307

Artioli, G., & Sarli, L. (2021). The qualitative method for a humanisation of research. *Acta Bio Medica: Atenei Parmensis*, *92*(Suppl. 2), Article e2021041. https://doi.org/10.23750%2Fabm.v92iS2.12042

Aslan, C., Kargın, A., & Şahin, M. (2020). Neutrosophic modeling of Talcott Parsons's action and decision-making applications for it. *Symmetry*, *12*(7), Article 1166. https://doi.org/10.3390/sym12071166

Aspers, P., & Corte, U. (2019). What is qualitative in qualitative research. *Qualitative Sociology*, *42*(2), 139–160. https://doi.org/10.1007/s11133-019-9413-7

Ayala, R. A., Koch, T. F., & Messing, H. B. (2019). The system of nursing in Chile: Insights from a systems theory perspective. *Nursing Inquiry*, *26*(1), Article e12260. https://doi.org/10.1111/nin.12260

Barker, W. C., Fisher, W., Scarfone, K., & Souppaya, M. (2022, February). *Ransomware risk management: A cybersecurity framework profile* (Internal Report No. 8374).

U.S. Department of Commerce, National Institute of Standards and Technology. https://doi.org/10.6028/nist.ir.8374

Battistoni, C., Giraldo Nohra, C., & Barbero, S. (2019). A systemic design method to approach future complex scenarios and research towards sustainability: A holistic diagnosis tool. *Sustainability*, *11*(16), 4458. https://doi.org/10.3390/su11164458

Baur, N. (2019). Linearity vs. circularity? On some common misconceptions on the differences in the research process in qualitative and quantitative research. *Frontiers in Education, 4*. https://doi.org/10.3389/feduc.2019.00053

Bautista, J. R., Zhang, Y., & Gwizdka, J. (2021). Healthcare professionals' acts of correcting health misinformation on social media. *International Journal of Medical Informatics*, *148*, 104375. https://doi.org/10.1016/j.ijmedinf.2021.104375

Beckett, G. H., & Kobayashi, M. (2020). A meta-study of an ethnographic research in a multicultural and multilingual community: negotiations, resources, and dilemmas. *American Journal of Qualitative Research*, *4*(1), 85-106. https://doi.org/10.29333/ajqr/8267

Bhamare, D., Zolanvari, M., Erbad, A., Jain, R., Khan, K., & Meskin, N. (2020). Cybersecurity for industrial control systems: a survey. *Computers & Security, 89*, 101677. https://doi.org/10.1016/j.cose.2019.101677

Bhuyan, S. S., Kabir, U. Y., Escareno, J. M., Ector, K., Palakodeti, S., Wyant, D., Kumar, S., Levy, M., Kedia, S., Dasgupta, D., & Dobalian, A. (2020). Transforming healthcare cybersecurity from reactive to proactive: Current status and future

recommendations. *Journal of Medical Systems*, *44*(5). https://doi.org/10.1007/s10916-019-1507-y

Bier, V., & Gutfraind, A. (2019). Risk analysis beyond vulnerability and resilience - characterizing the defensibility of critical systems. *European Journal of Operational Research*, *276*(2), 626-636. https://doi.org/10.1016/j.ejor.2019.01.011

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

Branch, L. E., Eller, W. S., Bias, T. K., McCawley, M. A., Myers, D. J., Gerber, B. J., & Bassler, J. R. (2019). Trends in malware attacks against United States healthcare organizations, 2016-2017. *Global Biosecurity*, *1*(1), 15. https://doi.org/10.31646/gbio.7

Braun, V., & Clarke, V. (2021). To saturate or not to saturate? Questioning data saturation as a useful concept for thematic analysis and sample-size rationales. *Qualitative Research in Sport, Exercise and Health*, *13*(2), 201-216. https://doi.org/10.1080/2159676X.2019.1704846

Brown, A., & Danaher, P. A. (2019). CHE principles: Facilitating authentic and dialogical semi-structured interviews in educational research. *International Journal of Research & Method in Education*, *42*(1), 76-90. https://doi.org/10.1080/1743727X.2017.1379987

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*, 101776. https://arxiv.org/pdf/2003.07674.pdf

Busetto, L., Wick, W., & Gumbinger, C. (2020). How to use and assess qualitative research methods. *Neurological Research and Practice, 2*(1). https://doi.org/10.1186/s42466-020-00059-z

Caster, M. (2020). Policies and procedures in providing competent customer service in urgent care centers. *Open Journal of Business and Management*, *08*(03), 1164-1192. https://doi.org/10.4236/ojbm.2020.83075

Chai, K. Y., & Zolkipli, M. F. (2021). Review on confidentiality, integrity, and availability in information security. *Journal of ICT in Education, 8*(2), 34-42. https://doi.org/10.37134/jictie.vol8.2.4.2021

Chan, C.-T., & Chen, H.-W. (2022). Impact of COVID-19 on the tourism industry in Taiwan. *Sustainability*, *14*(8), 4864. https://doi.org/10.3390/su14084864

Chatterjee, S., Sarker, S., Lee, M. J., Xiao, X., & Elbanna, A. (2021). A possible conceptualization of the information systems (IS) artifact: A general systems theory perspective. *Information Systems Journal*, *31*(4), 550-578. https://doi.org/10.1111/isj.12320

Chikere, C., & Nuwoka, J. (2015). The systems theory of management in modern day organizations - a study of Aldgate congress resort limited port harcourt. *International Journal of Scientific and Research Publications*. *5*(9). https://www.ijsrp.org/research-paper-0915/ijsrp-p4554.pdf

Chung, M. (2019). Why employees matter in the fight against ransomware. *Computer Fraud & Security, 2019*(8), 8-11. https://doi.org/10.1016/S1361-3723(19)30084-3

Chung, M. (2020). New ransomware innovations bring shame and fear to healthcare. *Journal of Healthcare Compliance, 22*(5), 37–63. https://search.ebscohost.com/login.aspx?direct=true&AuthType=shib&db=bth&AN=146114433&site=eds-live&scope=site&custid=s6527200

Churchman, C. W. (1970). Operations research as a profession. *Management Science, 17*(2), B-37-B-53. https://doi.org/10.1287/mnsc.17.2.b37

Collingridge, D. S., & Gantt, E. E. (2008). The quality of qualitative research. *American Journal of Medical Quality, 23*(5), 389-395. https://doi.org/10.1177/1062860608320646

Computer Security Research Center. (2021). Ransomware protection and response. NIST. https://csrc.nist.gov/Projects/ransomware-protection-and-response

Connolly, L. Y., & Wall, D. S. (2019). The rise of crypto-ransomware in a changing cybercrime landscape: Taxonomising countermeasures. *Computers & Security*, *87*, 101568. https://doi.org/10.1016/j.cose.2019.101568

Coutts, K. A., & Solomon, M. (2020). The use of diet modifications and third-party disability in adult dysphagia: The unforeseen burden of caregivers in an economically developing country. *South African Journal of Communication Disorders*, *67*(1). https://doi.org/10.4102/sajcd.v67i1.777

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

CUI Weicheng. (2021). On the philosophical ontology for a general system theory. *Philosophy Study, 11*(6). https://doi.org/10.17265/2159-5313/2021.06.002

Cybersecurity & Infrastructure Security Agency. (2019, August 21). CISA insights - ransomware outbreak. *CISA.gov*. https://www.cisa.gov/blog/2019/08/21/cisa-insights-ransomware-outbreak-0

Cybersecurity and Infrastructure Security Agency, the Federal Bureau of Investigation, & the Department of Health and Human Services. (2020, October 28). *Ransomware activity targeting the healthcare and public health sector* (Alert No. AA20-302A). https://us-cert.cisa.gov/ncas/alerts/aa20-302a

Daniel, B. K. (2019). Using the TACT framework to learn the principles of rigour in qualitative research. *Electronic Journal of Business Research Methods, 17*(3). https://doi.org/10.34190/jbrm.17.3.002

Danley, S. (2021). An activist in the field: social media, ethnography, and community. *Journal of Urban Affairs, 43*(3), 397-413. https://doi.org/10.1080/07352166.2018.1511797

Da Veiga, A., Astakhova, L. V., Botha, A., & Herselman, M. (2020). Defining organisational information security culture—Perspectives from academia and industry. *Computers & Security, 92*, 101713. https://doi.org/10.1016/j.cose.2020.101713

Davies, S. R., Macfarlane, R., & Buchanan, W. J. (2021). Differential area analysis for ransomware attack detection within mixed file datasets. *Computers & Security, 108*, 102377. https://doi.org/10.1016/j.cose.2021.102377

Dawadi, S., Shrestha, S., & Giri, R. A. (2021). Mixed-methods research: a discussion on its types, challenges, and criticisms. *Journal of Practical Studies in Education*, *2*(2), 25-36. https://doi.org/10.46809/jpse.v2i2.20

DeJonckheere, M., & Vaughn, L. M. (2019). Semistructured interviewing in primary care research: a balance of relationship and rigour. *Family medicine and community health*, *7*(2), e000057. https://doi.org/10.1136/fmch-2018-000057

Denton, M., Borrego, M., & Boklage, A. (2020). Community cultural wealth in science, technology, engineering, and mathematics education: A systematic review. *Journal of Engineering Education*, *109*(3), 556-580. https://doi.org/10.1002/jee.20322

Du, J., Raza, S. H., Ahmad, M., Alam, I., Dar, S. H., & Habib, M. A. (2022). Digital Forensics as Advanced Ransomware Pre-Attack Detection Algorithm for Endpoint Data Protection. *Security and Communication Networks*, *2022*, 1-16. https://doi.org/10.1155/2022/1424638

Eichelberg, M., Kleber, K., & Kämmerer, M. (2020). Cybersecurity challenges for PACS and medical imaging. *Academic Radiology*, *27*(8), 1126-1139. https://doi.org/10.1016/j.acra.2020.03.026

Evans, M., He, Y., Maglaras, L., & Janicke, H. (2019). HEART-IS: A novel technique for evaluating human error-related information security incidents. *Computers & Security*, *80*, 74-89. https://doi.org/10.1016/j.cose.2018.09.002

Ezer, F., & Aksüt, S. (2021). Opinions of graduate students of social studies education about qualitative research method. *International Education Studies, 14*(3), 15. https://doi.org/10.5539/ies.v14n3p15

Farrugia, B. (2019). WASP (write a scientific paper): Sampling in qualitative research. *Early Human Development, 133*, 69-71. https://doi.org/10.1016/j.earlhumdev.2019.03.016

Ferrando, M., Hoogerwerf, E.-J., & Kadyrbaeva, A. (2019). Qualitative research on the factors affecting transferability of digital solutions for integrated care. *International Journal of Integrated Care, 19*(4), 236. https://doi.org/10.5334/ijic.s3236

Filipec, O., & Plášil, D. (2021). The cybersecurity of healthcare. *Obrana a Strategie (Defence and Strategy), 21*(1), 27-52. https://doi.org/10.3849/1802-7199.21.2021.01.027-052

Fisher, R., Porod, C., & Peterson, S. (2021). Motivating employees and organizations to adopt a cybersecurity-focused culture. *Journal of Organizational Psychology*, *21*(1), 114-131. https://doi.org/10.33423/jop.v21i1.4030

FitzPatrick, B. (2019). Validity in qualitative health education research. *Currents in Pharmacy Teaching and Learning*, *11*(2), 211-217. https://doi.org/10.1016/j.cptl.2018.11.014)

Fofana, F., Bazeley, P., & Regnault, A. (2020). Applying a mixed methods design to test saturation for qualitative data in health outcomes research. *PloS one*, *15*(6), e0234898. https://doi.org/10.1371/journal.pone.0234898

Folami, F., Olowe, A., & Olugbade, J. (2019). Factors affecting the use of nursing process in Lagos University Teaching Hospital, Lagos, Nigeria. *International Journal of Africa Nursing Sciences, 10*, 26-30. https://doi.org/10.1016/j.ijans.2018.12.001

Fons-Martinez, J., Ferrer-Albero, C., & Diez-Domingo, J. (2022). Keys to improving the informed consent process in research: Highlights of the i-CONSENT project. *Health Expectations: An International Journal of Public Participation in Healthcare and Health Policy*, *25*(4), 1183. https://doi.org/10.1111%2Fhex.13427

Gill, S. L. (2020). Qualitative sampling methods. *Journal of Human Lactation, 36*(4), 579-581. https://doi.org/10.1177/0890334420949218

Gonul Kochan, C., Nowicki, D. R., Sauser, B., & Randall, W. S. (2018). Impact of cloud-based information sharing on hospital supply chain performance: A system dynamics framework. *International Journal of Production Economics, 195*, 168-185. https://doi.org/10.1016/j.ijpe.2017.10.008

Guest, G., Namey, E., & Chen, M. (2020). A simple method to assess and report thematic saturation in qualitative research. *PloS one*, *15*(5), e0232076. https://doi.org/10.1371/journal.pone.0232076

Guillain, A., Moncany, A.-H., Hamel, O., Gerson, C., Bougeard, R., Dran, G., & Debono, B. (2020). Spine neurosurgeons facing the judicialization of their profession: disenchantment and alteration of daily practice—a qualitative study. *Acta Neurochirurgica*, *162*(6), 1379-1387. https://doi.org/10.1007/s00701-020-04302-z

Haried, P., Claybaugh, C., & Dai, H. (2019). Evaluation of health information systems research in information systems research: A meta-analysis. *Health Informatics Journal, 25*(1), 186-202. https://doi.org/10.1177/1460458217704259

Hayat, A. A., Keshavarzi, M. H., Zare, S., Bazrafcan, L., Rezaee, R., Faghihi, S. A., Amini, M., & Kojuri, J. (2021). Challenges and opportunities from the COVID-19 pandemic in medical education: a qualitative study. *BMC Medical Education, 21*(1). https://doi.org/10.1186/s12909-021-02682-z

Heiselberg, L., & Stępińska, A. (2022). Transforming qualitative interviewing techniques for video conferencing platforms. *Digital Journalism*, 1-12. https://doi.org/10.1080/21670811.2022.2047083

Hennink, M., & Kaiser, B. N. (2022). Sample sizes for saturation in qualitative research: A systematic review of empirical tests. *Social Science & Medicine, 292*, 114523. https://doi.org/10.1016/j.socscimed.2021.114523

Hennink, M., Kaiser, B. N., & Weber, M. B. (2019). What influences saturation? Estimating sample sizes in focus group research. *Qualitative Health Research, 29*(10), 1483-1496. https://doi.org/10.1177/1049732318821692

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

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

Hu, S., Hsu, C., & Zhou, Z. (2021). The impact of SETA event attributes on employees' security-related Intentions: An event system theory perspective. *Computers & Security, 109*, 102404. https://doi.org/10.1016/j.cose.2021.102404

Hughes-Lartey, K., Li, M., Botchey, F. E., & Qin, Z. (2021). Human factor, a critical weak point in the information security of an organization's Internet of things. *Heliyon, 7*(3). https://doi.org/10.1016/j.heliyon.2021.e06522

Hull, G., John, H., & Arief, B. (2019). Ransomware deployment methods and analysis: views from a predictive model and human responses. *Crime Science, 8*(1). https://doi.org/10.1186/s40163-019-0097-9

Humayun, M., Jhanjhi, N., Alsayat, A., & Ponnusamy, V. (2021). Internet of things and ransomware: Evolution, mitigation and prevention. *Egyptian Informatics Journal, 22*(1), 105-117. https://doi.org/10.1016/j.eij.2020.05.003

Husband, G. (2020). Ethical data collection and recognizing the impact of semi-structured interviews on research respondents. *Education Sciences, 10*(8), 206. https://doi.org/10.3390/educsci10080206

Ibbett, H., & Brittain, S. (2020). Conservation publications and their provisions to protect research participants. *Conservation Biology*, *34*(1), 80-92. https://doi.org/10.1111/cobi.13337

Islam, M. A., & Aldaihani, F. M. F. (2022). Justification for adopting qualitative research method, research approaches, sampling strategy, sample size, interview method, saturation, and data analysis. *Journal of International Business and Management*, *5*(1), 01-11. https://doi.org/10.37227/JIBM-2021-09-1494

Jackson, M. C., & Sambo, L. G. (2020). Health systems research and critical systems thinking: the case for partnership. *Systems Research and Behavioral Science, 37*(1), 3–22. https://doi.org/10.1002/sres.2638

Jiménez, T. R., & Orozco, M. (2021). Prompts, not questions: four techniques for crafting better interview protocols. *Qualitative Sociology*, *44*(4), 507-528. https://doi.org/10.1007/s11133-021-09483-2

Johnson, J. L., Adkins, D., & Chauvin, S. (2020). A review of the quality indicators of rigor in qualitative research. *American Journal of Pharmaceutical Education*, *84*(1), 7120. https://doi.org/10.5688/ajpe7120

Johnson, M., Campbell, L., Svendsen, E., & McMillen, H. (2019). Mapping urban park cultural ecosystem services: a comparison of Twitter and semi-structured interview methods. *Sustainability, 11*(21), 6137. https://doi.org/10.3390/su11216137

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

Jung, Y., & Vakharia, N. (2019). Open systems theory for arts and cultural organizations: Linking structure and performance. *The Journal of Arts Management, Law, and Society*, *49*(4), 257-273. https://doi.org/10.1080/10632921.2019.1617813

Kakadellis, S., Woods, J., & Harris, Z. M. (2021). Friend or foe: Stakeholder attitudes towards biodegradable plastic packaging in food waste anaerobic digestion. *Resources, Conservation and Recycling*, *169*, 105529. https://doi.org/10.1016/j.resconrec.2021.105529

Karapapas, C., Pittaras, I., Fotiou, N., & Polyzos, G. C. (2020). Ransomware as a service using smart contracts and IPFS. 2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC). https://doi.org/10.1109/icbc48266.2020.9169451

Karavadra, B., Stockl, A., Prosser-Snelling, E., Simpson, P., & Morris, E. (2020). Women's perceptions of COVID-19 and their healthcare experiences: a qualitative thematic analysis of a national survey of pregnant women in the United Kingdom. *BMC Pregnancy and Childbirth*, *20*(1), 1-8. https://doi.org/10.1186/s12884-020-03283-2

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

Kessler, S. R., Pindek, S., Kleinman, G., Andel, S. A., & Spector, P. E. (2020). Information security climate and the assessment of information security risk among healthcare employees. *Health Informatics Journal*, *26*(1), 461-473. https://doi.org/10.1177/1460458219832048

Khayer, A., Bao, Y., & Nguyen, B. (2020). Understanding cloud computing success and its impact on firm performance: an integrated approach. *Industrial Management & Data Systems*, *120*(5), 963–985. https://doi.org/10.1108/IMDS-06-2019-0327

Kiser, S., & Maniam, B. (2021). Ransomware: healthcare industry at risk. *Journal of Business and Accounting*, *14*(1), 64-81. http://asbbs.org/files/2021-22/JBA_14.1_Fall_2021.pdf#page=65

Klose, M., Desai, V., Song, Y., & Gehringer, E. (2020). EDM and Privacy: Ethics and Legalities of Data Collection, Usage, and Storage. *International Educational Data Mining Society*. https://eric.ed.gov/?id=ED607820

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

Koçoglu, E., & Tekdal, D. (2020). Analysis of distance education activities conducted during COVID-19 pandemic. *Educational Research and Reviews*, *15*(9), 536-543. https://doi.org/10.5897/ERR2020.4033

Kraus, S., Breier, M., & Dasí-Rodríguez, S. (2020). The art of crafting a systematic literature review in entrepreneurship research. *International Entrepreneurship and*

Management Journal, 16(3), 1023-1042. https://doi.org/10.1007/s11365-020-00635-4

Kraus, S., Mahto, R. V., & Walsh, S. T. (2021). The importance of literature reviews in small business and entrepreneurship research. *Journal of Small Business Management*, 1-12. https://doi.org/10.1080/00472778.2021.1955128

Kritzinger, E., Da Vega, A., & van Staden, W. (2022). Measuring organizational information security awareness in South Africa. *Information Security Journal: A Global Perspective*, 1-14. https://doi.org/10.1080/19393555.2022.2077265

Kuek, A., & Hakkennes, S. (2020). Healthcare staff digital literacy levels and their attitudes towards information systems. *Health Informatics Journal, 26*(1), 592-612. https://doi.org/10.1177/1460458219839613

Kumar, R., Pandey, A. K., Baz, A., Alhakami, H., Alhakami, W., Agrawal, A., & Khan, R. A. (2020). Fuzzy-based symmetrical multi-criteria decision-making procedure for evaluating the impact of harmful factors of healthcare information security. *Symmetry*, *12*(4), 664. https://doi.org/10.3390/sym12040664

Kumar, S., Biswas, B., Bhatia, M. S., & Dora, M. (2021). Antecedents for enhanced level of cyber-security in organisations. *Journal of Enterprise Information Management, 34*(6), 1597-1629. https://doi.org/10.1108/jeim-06-2020-0240

Kurniawati, E., & Aliman, M. (2020). Community based tourism (CBT) to establish blue economy and improve public welfare for fishing tourism development in Klatak beach, Tulungagung, Indonesia. *Geo Journal of Tourism and Geosites*, *31*(3), 979-986. https://doi.org/10.30892/gtg.31307--530

Kuzminykh, I., Ghita, B., Sokolov, V., & Bakhshi, T. (2021). Information security risk assessment. *Encyclopedia*, *1*(3), 602–617. https://doi.org/10.3390/encyclopedia1030050

Lai, S. S., Pagh, J., & Zeng, F. H. (2019). Tracing communicative patterns: A comparative ethnography across platforms, media and contexts. *Nordicom Review*, *40*(s1), 141-157. https://doi.org/10.2478/nor-2019-0019

Lapum, J., Bailey, A., St-Amant, O., Garmaise-Yee, J., Hughes, M., & Mistry, S. (2022). Equity, diversity, and inclusion in open educational resources: An interpretive description of students' perspectives. *Nurse Education Today, 116*, 105459. https://doi.org/10.1016/j.nedt.2022.105459

Lavassani, K. M., & Movahedi, B. (2021). Firm-level analysis of global supply chain network: Role of centrality on firm's performance. *International Journal of Global Business and Competitiveness*, *16*(2), 86-103. https://doi.org/10.1007/s42943-021-00026-8

Lazlo, A., & Krippner, S. (1998). Systems theories and a priori aspects of perception. *ElsevierScience*. 3, 47-74. https://www.academia.edu/713345/Systems_Theories_Their_origins_foundations_and_development

Lee, C. S., & Kim, D. (2022). Pathways to cybersecurity awareness and protection behaviors in South Korea. *Journal of Computer Information Systems*, 1-13. https://doi.org/10.1080/08874417.2022.2031347

Liang, H.-F., Wu, K.-M., & Wang, Y.-H. (2020). Nursing students' first-time experiences in pediatric clinical practice in Taiwan: A qualitative study. *Nurse Education Today, 91*, 104469. https://doi.org/10.1016/j.nedt.2020.104469

Lindgreen, A., Di Benedetto, C. A., & Beverland, M. B. (2021). How to write up case-study methodology sections. *Industrial Marketing Management, 96*, A7-A10. https://doi.org/10.1016/j.indmarman.2020.04.012

Lobe, B., Morgan, D., & Hoffman, K. A. (2020). Qualitative data collection in an era of social distancing. *International Journal of Qualitative Methods, 19*, 160940692093787. https://doi.org/10.1177/1609406920937875

Maarouf, H. (2019). Pragmatism as a supportive paradigm for the mixed research approach: Conceptualizing the ontological, epistemological, and axiological stances of pragmatism. *International Business Research, 12*(9), 1. https://doi.org/10.5539/ibr.v12n9p1

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

Mahat-Shamir, M., Neimeyer, R. A., & Pitcho-Prelorentzos, S. (2021). Designing in-depth semi-structured interviews for revealing meaning reconstruction after loss. *Death Studies, 45*(2), 83-90. https://doi.org/10.1080/07481187.2019.1617388

Maigida, A. M., Abdulhamid, S. I. M., Olalere, M., Alhassan, J. K., Chiroma, H., & Dada, E. G. (2019). Systematic literature review and metadata analysis of

ransomware attacks and detection mechanisms. *Journal of Reliable Intelligent Environments, 5*(2), 67-89. https://doi.org/10.1007/s40860-019-00080-3

Majeed, M. H. (2019). Pragmatist inquiry into consumer behaviour research. *Philosophy of Management, 18*(2), 189-201. https://doi.org/10.1007/s40926-018-0103-4

McGaha, K. K., & D'Urso, P. A. (2019). A non-traditional validation tool: using cultural domain analysis for interpretive phenomenology. *International Journal of Social Research Methodology, 22*(6), 585-598. https://doi.org/10.1080/13645579.2019.1621474

McGrath, C., Palmgren, P. J., & Liljedahl, M. (2019). Twelve tips for conducting qualitative research interviews. *Medical teacher, 41*(9), 1002-1006. https://doi.org/10.1080/0142159X.2018.1497149

Mele, C., Pels, J., & Polese, F. (2010). A brief review of systems theories and their managerial applications. *Service Science, 2*(1-2), 126-135. https://doi.org/10.1287/serv.2.1_2.126

Melis, G., Sala, E., & Zaccaria, D. (2022). Remote recruiting and video-interviewing older people: a research note on a qualitative case study carried out in the first Covid-19 Red Zone in Europe. *International Journal of Social Research Methodology, 25*(4), 477-482. https://doi.org/10.1080/13645579.2021.1913921

Melon, E., & Hernandez, W. (2020). Cybersecurity in the dental healthcare sector: the need of knowledge for small practitioners. *Issues in Information Systems, 21*(1). https://doi.org/10.48009/1_iis_2020_118-124

Meyer, R. M., & O'Brien-Pallas, L. L. (2010). Nursing services delivery theory: an open system approach: Nursing services delivery theory. *Journal of Advanced Nursing*, *66*(12), 2828-2838. https://doi.org/10.1111/j.1365-2648.2010.05449.x

Middaugh, D. J. (2021). Cybersecurity attacks during a pandemic: It is not just IT's job! *Medsurg Nursing*, *30*(1), 65–66. https://search.ebscohost.com/login.aspx?direct=true&AuthType=shib&db=edb&AN=148827592&site=eds-live&scope=site&custid=s6527200

Mihai, N. (2021). Disrupt medicine. *Journal of Biology and Medicine*, 019-022. https://doi.org/10.17352/jbm.000027

Miller, K., & Flint-Stipp, K. (2019). Preservice teacher burnout: Secondary trauma and self-care issues in teacher education. *Issues in Teacher Education*, *28*(2), 28-45. https://files.eric.ed.gov/fulltext/EJ1239631.pdf

Millum, J., & Garnett, M. (2019). How payment for research participation can be coercive. *The American Journal of Bioethics*, *19*(9), 21-31. https://doi.org/10.1080/15265161.2019.1630497

Mirick, R., & Wladkowski, S. (2019). Skype in qualitative interviews: participant and researcher perspectives. *The Qualitative Report*. https://doi.org/10.46743/2160-3715/2019.3632

Mohajan, H. K. (2020). Quantitative research: A successful investigation in natural and social sciences. *Journal of Economic Development, Environment and People*, *9*(4). https://doi.org/10.26458/jedep.v9i4.679

Mohammadi, F., Farjam, M., Gholampour, Y., Sohrabpour, M., Oshvandi, K., & Bijani, M. (2021). Caregivers' perception of the caring challenges in coronavirus crisis (COVID-19): a qualitative study. *BMC Nursing, 20*(1). https://doi.org/10.1186/s12912-021-00607-1

Möller, K. (2022). Populism and the political system: A critical systems theory approach to the study of populism. *Philosophy & Social Criticism*, 019145372210840. https://doi.org/10.1177/01914537221084003

Monat, J., Amissah, M., & Gannon, T. (2020). Practical applications of systems thinking to business. *Systems*, *8*(2), 14. https://doi.org/10.3390/systems8020014

Montesino, R., & Fenz, S. (2011). Information security automation: How far can we go?. 2011 Sixth International Conference on Availability, Reliability and Security. https://doi.org/10.1109/ares.2011.48

Moon, M. D. (2019). Triangulation: A method to increase validity, reliability, and legitimation in clinical research. *Journal of Emergency Nursing*, *45*(1), 103-105. https://doi.org/10.1016/j.jen.2018.11.004

Morgan, H. (2022). Conducting a qualitative document analysis. *The Qualitative Report, 27*(1), 64-77. https://doi.org/10.46743/2160-3715/2022.5044

Muthuppalaniappan, M., & Stevenson, K. (2021). Healthcare cyber-attacks and the COVID-19 pandemic: an urgent threat to global health. *International Journal for Quality in Healthcare, 33*(1). https://doi.org/10.1093/intqhc/mzaa117

Namey, E., Guest, G., O'Regan, A., Godwin, C. L., Taylor, J., & Martinez, A. (2022). How does qualitative data collection modality affect disclosure of sensitive

information and participant experience? Findings from a quasi-experimental study. *Quality & Quantity, 56*(4), 2341-2360. https://doi.org/10.1007/s11135-021-01217-4

Nasiri, S., Sadoughi, F., Tadayon, M., & Dehnad, A. (2019). Security requirements of internet of things-based healthcare system: a survey study. *Acta Informatica Medica, 27*(4), 253. https://doi.org/10.5455/aim.2019.27.253-258

Nassaji, H. (2020). Good qualitative research. *Language Teaching Research, 24*(4), 427-431. https://doi.org/10.1177/1362168820941288

National Commission for the Protection of Human Subjects in Biomedical and Behavioral Research. (1979). *The Belmont Report: Ethical principles and guidelines for the protection of human subject's research,* (45CFR46). https://www.hhs.gov/ohrp/sites/default/files/the-belmont-report-508c_FINAL.pdf

Natow, R. S. (2020). The use of triangulation in qualitative studies employing elite interviews. *Qualitative Research, 20*(2), 160-173. https://doi.org/10.1177/1468794119830077

Neubauer, B. E., Witkop, C. T., & Varpio, L. (2019). How phenomenology can help us learn from the experiences of others. *Perspectives on Medical Education, 8*(2), 90-97. https://doi.org/10.1007/s40037-019-0509-2

Newaz, A. I., Sikder, A. K., Rahman, M. A., & Uluagac, A. S. (2021). A survey on security and privacy issues in modern healthcare systems: Attacks and defenses. *ACM Transactions on Computing for Healthcare, 2*(3), 1-44. https://doi.org/10.1145/3453176

Nifakos, S., Chandramouli, K., Nikolaou, C. K., Papachristou, P., Koch, S., Panaousis, E., & Bonacina, S. (2021). Influence of human factors on cyber security within healthcare organisations: A systematic review. *Sensors, 21*(15), 5119. https://doi.org/10.3390/s21155119

Nord, J. H., Koohang, A., Floyd, K., & Paliszkiewicz, J. (2020). Impact of habits on information security policy compliance. *Issues in Information Systems*, *21*(3), 217-226. https://doi.org/10.48009/3_iis_2020_217-226

Novek, S., & Wilkinson, H. (2019). Safe and inclusive research practices for qualitative research involving people with dementia: A review of key issues and strategies. *Dementia*, *18*(3), 1042-1059. https://doi.org/10.1177/1471301217701274

Noyes, J., Booth, A., Moore, G., Flemming, K., Tunçalp, Ö., & Shakibazadeh, E. (2019). Synthesizing quantitative and qualitative evidence to inform guidelines on complex interventions: clarifying the purposes, designs and outlining some methods. *BMJ global health*, *4*(Suppl 1), e000893. https://doi.org/10.1136/bmjgh-2018-000893

Office of the National Coordinator for Health Information Technology (CNC). (2018). What privacy and security laws protect patients' health information?. *HealthIT.gov*. https://www.healthit.gov/faq/what-privacy-and-security-laws-protect-patients-health-information

Ohn, M., & Ohn, K.-M. (2020). An evaluation study on gamified online learning experiences and its acceptance among medical students. *Tzu Chi Medical Journal*, *32*(2), 211. https://doi.org/10.4103/tcmj.tcmj_5_19

Omoyiola, B. (2020). The evolution of information security measurement and testing. *IOSR Journal of Computer Engineering. 22*(3). 50-54. https://doi.org/10.9790/0661-2203025054

Ormerod, R. (2020). The history and ideas of sociological functionalism: Talcott Parsons, modern sociological theory, and the relevance for OR. *Journal of the Operational Research Society*, *71*(12), 1873-1899. https://doi.org/10.1080/01605682.2019.1640590

Padwal, K., Thomas, A., Howard, T., & Carr, M. (2019). Common lessons from disparate information security incidents: A whitepaper analysis. October. *(ISC)2 National Capital Region Chapter*. http://web.isc2ncrchapter.org/wp-content/uploads/2019/10/Common-Lessons-From-Disparate-InfoSec-Incidents.pdf

Panetto, H., Iung, B., Ivanov, D., Weichhart, G., & Wang, X. (2019). Challenges for the cyber-physical manufacturing enterprises of the future. *Annual Reviews in Control*, *47*, 200-213. https://doi.org/10.1016/j.arcontrol.2019.02.002

Parfitt, C. M., & Rose, A. L. (2020). Informal mentoring for aspiring school leaders: A phenomenological study. *Mentoring & Tutoring: Partnership in Learning*, *28*(3), 278-294. https://doi.org/10.1080/13611267.2020.1778837

Pell, B., Williams, D., Phillips, R., Sanders, J., Edwards, A., Choy, E., & Grant, A. (2020). Using visual timelines in telephone interviews: reflections and lessons learned from the star family study. *International Journal of Qualitative Methods, 19*, 160940692091367. https://doi.org/10.1177/1609406920913675

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

Post, C., Sarala, R., Gatrell, C., & Prescott, J. E. (2020). Advancing theory with review articles. *Journal of Management Studies*, *57*(2), 351-376. https://doi.org/10.1111/JOMS.12549

Poustilnik, S. (2021). Aleksandr Bogdanov's tektology: A proletarian science of construction. *Cultural Science Journal*, *13*(1), 140-151. https://doi.org/10.2478/csj-2021-0011

Quintão, C., Andrade, P., & Almeida, F. (2020). How to improve the validity and reliability of a case study approach? *Journal of Interdisciplinary Studies in Education*, *9*(2), 273-284. https://doi.org/10.32674/jise.v9i2.2026

Rakhmawati, D. M., & Priyana, J. (2019). A study on 21st century skills integration in the English textbook for senior high school. *JEES (Journal of English Educators Society)*, *4*(1), 9-16. https://doi.org/10.21070/jees.v4i1.1873

Ranganath, G. D., & Rajeshwaran, N. (2022). Quality of accounting information systems and organizational effectiveness in an emerging country. *SMART Journal of Business Management Studies*, *18*(1), 22-29. http://https/doi.org/10.5958/2321-2012.2022.00003.3

Ranieri, M., Giampaolo, M., & Bruni, I. (2019). Exploring educators' professional learning ecologies in a blended learning environment. *British Journal of Educational Technology*, *50*(4), 1673-1686. https://doi.org/10.1111/bjet.12793

Reich, J. (2021). Preregistration and registered reports. *Educational Psychologist*, *56*(2), 101-109. https://doi.org/10.1080/00461520.2021.1900851

Ren, A., Liang, C., Hyug, I., Broh, S., & Jhanjhi, N. (2018). A three-level ransomware detection and prevention mechanism. *EAI Endorsed Transactions on Energy Web, 0*(0), 162691. https://doi.org/10.4108/eai.13-7-2018.162691

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

Reshmi, T. R. (2021). Information security breaches due to ransomware attacks - a systematic literature review. *International Journal of Information Management Data Insights*, *1*(2), 100013. https://doi.org/10.1016/j.jjimei.2021.100013

Ribatti, D. (2021). Reductionism, vitalism, and holism. *Critical Reviews in Eukaryotic Gene Expression*, *31*(3), 1-3. https://doi.org/10.1615/critreveukaryotgeneexpr.2021037947

Richardson, R., North, M. M., & Garofalo, D. (2021). Ransomware: the landscape is shifting-a concise report. *International Management Review*, *17*(1), 5-86. http://www.americanscholarspress.us/journals/IMR/pdf/IMR-1-2021/V17n121-art1.pdf

Robinson, O. C. (2014). Sampling in interview-based qualitative research: A theoretical and practical guide. *Qualitative research in psychology*, *11*(1), 25-41. https://doi.org/10.1080/14780887.2013.801543

Rose, J., & Johnson, C. W. (2020). Contextualizing reliability and validity in qualitative research: toward more rigorous and trustworthy qualitative social science in leisure research. *Journal of Leisure Research*, *51*(4), 432-451. https://doi.org/10.1080/00222216.2020.1722042

Ruotsalainen, P., & Blobel, B. (2020). Health information systems in the digital health ecosystem—problems and solutions for ethics, trust and privacy. *International Journal of Environmental Research and Public Health, 17*(9), 3006. https://doi.org/10.3390/ijerph17093006

Safarov, N. (2021). Personal experiences of digital public services access and use: Older migrants' digital choices. *Technology in Society, 66*, 101627. https://doi.org/10.1016/j.techsoc.2021.101627

Sandar, A. M., Min, Y., & Win, K. M. N. (2019). Fundamental areas of cyber security on latest technology. *International Journal of Trend in Scientific Research and Development, 3*(5). https://doi.org/10.31142/ijtsrd26550

Santolini, J., Wootton, S. A., Jackson, A. A., & Feelisch, M. (2019). The Redox architecture of physiological function. *Current Opinion in Physiology, 9*, 34-47. https://doi.org/10.1016/j.cophys.2019.04.009

Savaş, S., & Karataş, S. (2022). Cyber governance studies in ensuring cybersecurity: an overview of cybersecurity governance. *International Cybersecurity Law Review*, *3*(1), 7-34. https://doi.org/10.1365/s43439-021-00045-4

Scalco, A., Flanigan, D., & Simske, S. (2021). Control systems cyber security reference architecture (RA) for critical infrastructure: Healthcare and hospital vertical example. *Journal of Critical Infrastructure Policy, 2*(2). https://doi.org/10.18278/jcip.2.2.7

Schriber, S., & Löwstedt, J. (2020). Reconsidering ordinary and dynamic capabilities in strategic change. *European Management Journal*, *38*(3), 377-387. https://doi.org/10.1016/j.emj.2019.12.006

Sebele-Mpofu, F. Y. (2020). Saturation controversy in qualitative research: Complexities and underlying assumptions. A literature review. *Cogent Social Sciences*, *6*(1). https://doi.org/10.1080/23311886.2020.1838706

Shalom, M., & Luria, E. (2019). The multi-age school structure: Its value and contributions in relation to significant learning. *Educational Practice and Theory*, *41*(1), 5-21. https://doi.org/10.7459/ept/41.1.02

Shi, C., Zhu, H., Liu, J., Zhou, J., & Tang, W. (2020). Barriers to self-management of type 2 diabetes during COVID-19 medical isolation: a qualitative study. *Diabetes, Metabolic Syndrome and Obesity: Targets and Therapy*, *13*, 3713. https://doi.org/10.2147%2FDMSO.S268481

Shi, Y., Zhai, G., Xu, L., Zhou, S., Lu, Y., Liu, H., & Huang, W. (2021). Assessment methods of urban system resilience: From the perspective of complex adaptive system theory. *Cities, 112*, 103141. https://doi.org/10.1016/j.cities.2021.103141

Shorey, S., & Ng, E. D. (2022). Examining characteristics of descriptive phenomenological nursing studies: A scoping review. *Journal of Advanced Nursing. (78)*7, 1968-1979. https://doi.org/10.1111/jan.15244

Siitonen, M., De la Hera, T., & Reer, F. (2021). Looking ahead in games research: Entry points into a pragmatic field of inquiry. *Media and Communication*, *9*(1), 1-4. https://doi.org/10.17645/mac.v9i1.3685

Šijan, A., Karabašević, D., & Rajčević, D. (2019). The importance of the general system theory for the modern world. *Trendovi u poslovanju*, *7*(2), 87-94. https://doi.org/10.5937/trendpos1902087q

Sim, J., & Waterfield, J. (2019). Focus group methodology: some ethical challenges. *Quality & Quantity*, *53*(6), 3003-3022. https://doi.org/10.1007/s11135-019-00914-5

Singh, A. N., & Gupta, M. P. (2019). Information Security Management Practices: Case Studies from India. *Global Business Review, 20*(1), 253-271. https://doi.org/10.1177/0972150917721836

Skjott Linneberg, M., & Korsgaard, S. (2019). Coding qualitative data: a synthesis guiding the novice, *Qualitative Research Journal*, (19) 3, 259-270. https://doi.org/10.1108/QRJ-12-2018-0012

Smith, B. G., Whiffin, C. J., Esene, I. N., Karekezi, C., Bashford, T., Mukhtar Khan, M., Fontoura Solla, D. J., Indira Devi, B., Hutchinson, P. J., Kolias, A. G., Figaji, A., & Rubiano, A. M. (2021). Neurotrauma clinicians' perspectives on the contextual challenges associated with long-term follow-up following traumatic brain injury in low-income and middle-income countries: a qualitative study protocol. *BMJ Open, 11*(3), e041442. https://doi.org/10.1136/bmjopen-2020-041442

Smith, M. G., Witte, M., Rocha, S., & Basner, M. (2019). Effectiveness of incentives and follow-up on increasing survey response rates and participation in field studies. *BMC medical research methodology*, *19*(1). https://doi.org/10.1186/s12874-019-0868-8

Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research*, *104*, 333-339. https://doi.org/10.1016/j.jbusres.2019.07.039

Souganidis, E. S., Patel, B., & Sampayo, E. M. (2022). Physician-specific utilization of an electronic best practice alert for pediatric sepsis in the emergency department. *Pediatric Emergency Care*, *38*(8), e1417-e1422. https://doi.org/10.1097/PEC.0000000000002778

Spannring, R., & Hawke, S. (2022). Anthropocene challenges for youth research: understanding agency and change through complex, adaptive systems. *Journal of Youth Studies*, *25*(7), 977-993. https://doi.org/10.1080/13676261.2021.1929886

Sridharan, V. G. (2021). Methodological Insights Theory development in qualitative management control: revisiting the roles of triangulation and

generalization. *Accounting, Auditing & Accountability Journal*, *34*(2), 451-479. https://doi.org/10.1108/AAAJ-09-2019-4177

Stahl, N. A., & King, J. R. (2020). Expanding approaches for research: Understanding and using trustworthiness in qualitative research. *Journal of Developmental Education*, *44*(1), 26-28. https://files.eric.ed.gov/fulltext/EJ1320570.pdf

Stenfors, T., Kajamaa, A., & Bennett, D. (2020). How to assess the quality of qualitative research. *The Clinical Teacher*, *17*(6), 596-599. https://doi.org/10.1111/tct.13242

Stevens, C. J., Horrigan, J., Heale, R., & Koren, I. (2020). Northeastern Ontario nurses' perceptions of e-learning: An interpretive description. *Nurse Education Today*, *92*, 104509. https://doi.org/10.1016/j.nedt.2020.104509

Sulistyowati, D., Handayani, F., & Suryanto, Y. (2020). Comparative analysis and design of cybersecurity maturity assessment methodology using NIST CSF, COBIT, ISO/IEC 27002 and PCI DSS. *JOIV: International Journal on Informatics Visualization*, *4*(4), 225-230. https://doi.org/10.30630/joiv.4.4.482

Sundler, A. J., Lindberg, E., Nilsson, C., & Palmér, L. (2019). Qualitative thematic analysis based on descriptive phenomenology. *Nursing Open*, *6*(3), 733-739. https://doi.org/10.1002/nop2.275

Tadros, E. (2020). The puzzling metaphor: teaching general systems theory to marriage and family therapy trainees. *The Family Journal*, *28*(1), 98–102. https://doi.org/10.1177/1066480719868702

Taherdoost, H. (2022). What are different research approaches? Comprehensive review of qualitative, quantitative, and mixed method research, their applications, types,

and limitations. *Journal of Management Science and Engineering Research, 5*(1). https://doi.org/10.30564/jmser.v5i1.4538

Tarafdar, P., & Bose, I. (2019). Systems theoretic process analysis of information security: the case of Aadhaar. *Journal of Organizational Computing and Electronic Commerce, 29*(3), 209–222. https://doi.org/10.1080/10919392.2019.1598608

Tarikere, S., Donner, I., & Woods, D. (2021). Diagnosing a healthcare cybersecurity crisis: the impact of IoMT advancements and 5G. *Business Horizons*, *64*(6), 799-807. https://doi.org/10.1016/j.bushor.2021.07.015

Thamer, N., & Alubady, R. (2021, April). A survey of ransomware attacks for healthcare systems: Risks, challenges, solutions and opportunity of research. In *2021 1st Babylon International Conference on Information Technology and Science (BICITS)* (pp. 210-216). IEEE. https://doi.org/10.1109/BICITS51482.2021.9509877

Thompson, E. C. (2020). HIPAA security rule and cybersecurity operations. *designing a HIPAA-compliant security operations center*, 23-36. https://doi.org/10.1007/978-1-4842-5608-4_2

Thorne, S. (2016). *Interpretive description: Qualitative research for applied practice (2nd ed.)*. Routledge. https://doi.org/10.4324/9781315545196

Thunberg, S., & Arnell, L. (2021). Pioneering the use of technologies in qualitative research – A research review of the use of digital interviews. *International*

Journal of Social Research Methodology. *25*(6), 757-768, https://doi.org/10.1080/13645579.2021.1935565

Tiidenberg, K. (2020). Research ethics, vulnerability, and trust on the internet. *Second international handbook of internet research*, 569-583. https://doi.org/10.1007/978-94-024-1555-1_55

Tomaszewski, L. E., Zarestky, J., & Gonzalez, E. (2020). Planning qualitative research: Design and decision making for new researchers. *International Journal of Qualitative Methods*, *19*, 1609406920967174. https://doi.org/10.1177/1609406920967174

Topa, I., & Karyda, M. (2019). From theory to practice: guidelines for enhancing information security management. *Information & Computer Security*, *27*(3), 326-342. https://doi.org/10.1108/ICS-09-2018-0108

Tretter, F. (2019). "Systems medicine" in the view of von Bertalanffy's "organismic biology" and systems theory. *Systems Research and Behavioral Science*, *36*(3), 346-362. https://doi.org/10.1002/sres.2588

Tretter, F., Wolkenhauer, O., Meyer-Hermann, M., Dietrich, J. W., Green, S., Marcum, J., & Weckwerth, W. (2021). The quest for system-theoretical medicine in the COVID-19 era. *Frontiers in Medicine, 8*. https://doi.org/10.3389/fmed.2021.640974

Tully, J., Selzer, J., Phillips, J. P., O'Connor, P., & Dameff, C. (2020). Healthcare challenges in the era of cybersecurity. *Health Security, 18*(3), 228-231. http://doi.org/10.1089/hs.2019.0123

Turner, J. R., & Baker, R. M. (2019). Complexity theory: An overview with potential applications for the social sciences. *Systems, 7*(1), 4. https://doi.org/10.3390/systems7010004

Uandykova, M., Lisin, A., Stepanova, D., Baitenova, L., Mutaliyeva, L., Yüksel, S., & Dincer, H. (2020). The social and legislative principles of counteracting ransomware crime. *Entrepreneurship and Sustainability Issues*. http://doi.org/10.9770/jesi.2020.8.2(47)

Upadhyay, D., & Sampalli, S. (2020). SCADA (Supervisory Control and Data Acquisition) systems: Vulnerability assessment and security recommendations. *Computers & Security*, *89*, 101666. https://doi.org/10.1016/j.cose.2019.101666

U.S. Department of Health & Human Services, Office of Information Security. (2021, February 18). *2020: A retrospective look at healthcare cybersecurity* (Report No. 202102181030). https://www.hhs.gov/sites/default/files/2020-hph-cybersecurty-retrospective-tlpwhite.pdf

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

Van Assche, K., Verschraegen, G., Valentinov, V., & Gruezmacher, M. (2019b). The social, the ecological, and the adaptive. Von Bertalanffy's general systems theory

and the adaptive governance of social-ecological systems. *Systems Research and Behavioral Science, 36*(3), 308-321. https://doi.org/10.1002/sres.2587

Vindrola-Padros, C., Chisnall, G., Cooper, S., Dowrick, A., Djellouli, N., Symmons, S. M., Martin, S., Singleton, G., Vanderslott, S., Vera, N., & Johnson, G. A. (2020). Carrying out rapid qualitative research during a pandemic: emerging lessons from COVID-19. *Qualitative Health Research, 30*(14), 2192-2204. https://doi.org/10.1177/1049732320951526

von Bertalanffy, L. (1951). Theoretical models in biology and psychology. *Journal of Personality, 20*(1), 24-38. https://doi.org/10.1111/j.1467-6494.1951.tb01511.x

von Bertalanffy, L. (1968). *General system theory: foundations, development, applications*. George Braziller.

von Bertalanffy, L., & Sutherland, J. W. (1974). General systems theory: foundations, developments, applications. *IEEE Transactions on Systems, Man, and Cybernetics, SMC-4*(6), 592-592. https://doi.org/10.1109/tsmc.1974.4309376

Waalkes, P. L., Hall, D., Swindle, P. J., & Haugen, J. E. S. (2021). Beginning counselor educators' experiences of teaching mentorship. *Teaching and Supervision in Counseling*. https://doi.org/10.7290/tsc030108

Wainwright, E., Looseley, A., Mouton, R., O'Connor, M., Taylor, G., Cook, T. M., & SWEAT Study Investigator Group. (2019). Stress, burnout, depression, and work satisfaction among UK anesthetic trainees: a qualitative analysis of in-depth participant interviews in the satisfaction and wellbeing in anesthetic training study. *Anesthesia, 74*(10), 1240-1251. https://doi.org/10.1111/anae.14694

Walton, J. (2021). The entanglement of scientism, neoliberalism and materialism. *Paradigm Explorer*, (2021/1), 8-12. http://ray.yorksj.ac.uk/id/eprint/5397/

Wan, M., Li, J., Liu, Y., Zhao, J., & Wang, J. (2021). Characteristic insights on industrial cyber security and popular defense mechanisms. *China Communications*, *18*(1), 130-150. https://doi.org/10.23919/JCC.2021.01.012

Watson, S. L., & Watson, W. R. (2011). Critical, emancipatory, and pluralistic research for education: A review of critical systems theory. *Journal of Thought, 46*(3-4), 63. https://doi.org/10.2307/jthought.46.3-4.63

Watson, S. L., & Watson, W. R. (2013). Chapter six: Critical systems theory for qualitative research methodology. *Counterpoints, 354*, 111–127. http://www.jstor.org/stable/42981166

Weber, R. (2020). Taking the ontological and materialist turns: Agential realism, representation theory, and accounting information systems. *International Journal of Accounting Information Systems, 39*, 100485. https://doi.org/10.1016/j.accinf.2020.100485

Williams, H. (2021). The meaning of "phenomenology": Qualitative and philosophical phenomenological research methods. *The Qualitative Report*. https://doi.org/10.46743/2160-3715/2021.4587

Williams, T., Wiles, J., Smith, M., & Ward, K. (2022). Combining action research and grounded theory in health research: A structured narrative review. *SSM - Qualitative Research in Health, 2*, 100093. https://doi.org/10.1016/j.ssmqr.2022.100093

Wolff, B., Mahoney, F., Lohiniva, A. L., & Corkum, M. (2019). Collecting and analyzing qualitative data. *The CDC Field Epidemiology Manual*, 213-228. https://doi.org/10.1093/oso/9780190933692.003.0010

Wu, Z., & Trigo, V. (2021). Impact of information system integration on the healthcare management and medical services. *International Journal of Healthcare Management, 14*(4), 1348-1356. https://doi.org/10.1080/20479700.2020.1760015

Wymer, J. A., Weberg, D. R., Stucky, C. H., & Allbaugh, N. N. (2023). Human-centered design: principles for successful leadership across healthcare teams and technology. *Nurse Leader, 21*(1), 93-98. https://doi.org/10.1016/j.mnl.2022.11.004

Xin, X., Shu-Jiang, Y., Nan, P., ChenXu, D., & Dan, L. (2022). Review on a big data-based innovative knowledge teaching evaluation system in universities. *Journal of Innovation & Knowledge, 7*(3), 100197. https://doi.org/10.1016/j.jik.2022.100197

Xu, A., Baysari, M. T., Stocker, S. L., Leow, L. J., Day, R. O., & Carland, J. E. (2020). Researchers' views on, and experiences with, the requirement to obtain informed consent in research involving human participants: a qualitative study. *BMC Medical Ethics, 21*(1), 1-11. https://doi.org/10.1186/s12910-020-00538-7

Yan, J., Feng, L., Denisov, A., Steblyanskaya, A., & Oosterom, J.-P. (2020). Complexity theory for the modern Chinese economy from an information entropy perspective: Modeling of economic efficiency and growth potential. *PLOS ONE, 15*(1), e0227206. https://doi.org/10.1371/journal.pone.0227206

Zairul, M. (2021). Can member check be verified in real time? Introducing arc (asking, record, confirm) for member checking validation strategy in qualitative research. *Engineering Journal*, *25*(1), 245-251. https://doi.org/10.4186/ej.2021.25.1.245

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2022). Cyber security awareness, knowledge and behavior: A comparative study. *Journal of Computer Information Systems*, *62*(1), 82-97. https://doi.org/10.1080/08874417.2020.1712269

Appendix A: Human Subjects Research Training Completion

CITI PROGRAM

Completion Date 24-Jan-2021
Expiration Date N/A
Record ID 40526401

This is to certify that:

Alejandro Ruiz

Not valid for renewal of certification through CME.

Has completed the following CITI Program course:

Student's
(Curriculum Group)
Doctoral Student Researchers
(Course Learner Group)
1 - Basic Course
(Stage)

Under requirements set by:

Walden University

CITI
Collaborative Institutional Training Initiative

Verify at www.citiprogram.org/verify/?web11909a-4fe8-4c86-bf39-5f6d01def8b1-40526401

Appendix B: Interview Protocol and Questions

1. What cybersecurity strategies have you used to protect your healthcare organizations (HCOs) from ransomware attacks?
2. Have you participated in protecting information systems against a ransomware attack that accessed part or all the organizational healthcare information system (HIS) or patient health information (PHI)? Please describe this experience.
3. How do these ransomware attacks help shape current established cybersecurity strategies in your organization? Please describe the experience and elaborate on your response.
4. How do cybersecurity strategies fit into your organization as a whole?
5. How can you improve current cybersecurity strategies to protect IS better from ransomware cyberattacks?
6. What are the key barriers to implementing better strategies to protect IS from ransomware cyberattacks?
7. What are the frequent cybersecurity fail areas of IS guidelines & strategies regarding ransomware cyberattacks? Why?
8. What are the frequent cybersecurity success areas of IS guidelines & strategies regarding ransomware cyberattacks? Why?
9. What importance do external factors such as laws and regulations play in establishing cybersecurity strategies to protect IS from ransomware attacks in your organization? Why?

10. Which additional cybersecurity strategies would you implement to protect IS from ransomware cyberattacks? Why?

Interview Protocol for the Study: Cybersecurity Strategies IT Managers Use to Protect Healthcare Information Systems From Ransomware

Date of Interview:_____ Study Participant:_____

Duration of Interview: _____ Interview #:_____

Interview

A. An email invitation to participants, located in Appendix C, will help establish the study's intent between participants and the researcher.
B. The interview questions, located in Appendix B, will also be presented to all participants for their review before the interview.
C. A videoconference interview will take place focusing on the exploration of strategies used by IT leaders in healthcare organizations (HCOs) to protect information systems (IS) from ransomware cyberattacks.
D. During the semi-structured interview, I will show my appreciation to each participant for fulfilling the research's invitation to participate.
E. Participants will be reminded at the start of the interview that the process will require the use of a digital recorder, while having a full charged cellphone as a backup recording device.
F. The recorder and its backup recording device are turned on once consent is received from the participants.

G. The researcher will not include any personal identifiers in the report such as your name, job, place of work, or any other information that could help identify you in any of the study reports.

H. Participants may stop the interview at any moment.

I. The researcher will emphasize on the participant's perspectives while evaluating the emerging of any new topics that were previously not specified in the interview questions.

J. Each interview session lasts approximately 30 to 40 minutes until all questions have been answered.

K. Before concluding the interview sessions, I will ask if they wish to add any relevant data they wish to contribute.

L. The member checking process will be explained to the participant when the interview session concludes.

M. Schedule the follow up interview from member checking to confirm my interpretation of the interviewee's words, after conducting the bulleted summary of the transcribed interview.

N. The interview session will end with a thank you note for participation, reminding of a future 15-minute follow-up interview, once all question responses have been confirmed to the satisfaction of the participants.

O. Before the recorders are turned off, a reminder to participants will be made stating that they will receive a copy of the finding's interpretation later on for their review.

Follow-Up Interview

Script: I would like to have the opportunity for a 15-minute follow-up recorded videoconference interview to review my interpretation to the interview answers while also offering you the chance to rectify any errors or provide additional information if deemed fit. I will refer the participants to the bulleted summary of my interpretation of their response, asking if the interpretation coincides with their responses point of view. I will use this form to document the participants reactions and comments on the interpretation as part of the study field notes.

Interview Questions	**Was the answer interpreted accurately and reflected the intended answer? Is there any additional information to contribute?**
1. What cybersecurity strategies have you used to protect your healthcare organizations from ransomware attacks?	**Interpretation:** **Comments:**
2. Have you participated in protecting information systems against a ransomware attack that accessed part or all the organizational healthcare information system (HIS) or patient	**Interpretation:** **Comments:**

health information (PHI)? Please describe this experience.	
3. How do these ransomware attacks help shape current established cybersecurity strategies in your organization? Please describe the experience and elaborate on your response.	**Interpretation:** **Comments:**
4. How do cybersecurity strategies fit into your organization as a whole?	**Interpretation:** **Comments:**
5. How can you improve current cybersecurity strategies to protect IS better from ransomware cyberattacks?	**Interpretation:** **Comments:**
6. What are the key barriers to implementing better strategies to protect IS from ransomware cyberattacks?	**Interpretation:** **Comments:**
7. What are the frequent cybersecurity fail areas of IS guidelines & strategies regarding ransomware cyberattacks? Why?	**Interpretation:** **Comments:**

8. What are the frequent cybersecurity success areas of IS guidelines & strategies regarding ransomware cyberattacks? Why?	**Interpretation:** **Comments:**
9. What importance do external factors such as laws and regulations play in establishing cybersecurity strategies to protect IS from ransomware attacks in your organization? Why?	**Interpretation:** **Comments:**
10. Which additional cybersecurity strategies would you implement to protect IS from ransomware cyberattacks? Why?	**Interpretation:** **Comments:**

Appendix C: Invitation to Healthcare Organization Information Technology Leaders

Dear <IT leader's name>,

I am Alejandro Ruiz Caíno, student in the Doctorate in Information Technology program at Walden University. I am conducting interviews as part of a research study to understand the strategies IT leaders in healthcare organizations (HCO's) use to protect information systems (IS) from ransomware cyberattacks. I am kindly asking you to participate in a 30-min interview.

The study participants will receive a $20 gift card as compensation for participation. Your involvement may contribute to cybersecurity knowledge on HCOs information technology ransomware protection strategies. I will present you with a link to the report of the study's findings, after it has been accepted for publication. Please review the attached Informed Consent Form for more details about privacy and confidentiality. If you feel you understand the study and wish to volunteer, please indicate your consent by replying to this email with the words "I consent."

Thanks in advance for your help and prompt response to this request. If you have any questions, contact me at my cellphone at [telephone number redacted] or [email address redacted].

Best regards,

Alejandro Ruiz Caino, MBA

Doctoral Candidate, Doctor of Information Technology

Walden University