Walden University
ScholarWorks

Walden Dissertations and Doctoral Studies

Walden Dissertations and Doctoral Studies Collection

2021

Mitigating IT Security Risk in United States Healthcare: A Qualitative Examination of Best Practices

JoAnn Hemann
Walden University

Walden University

College of Management and Technology

This is to certify that the doctoral dissertation by

JoAnn Hemann

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. Danielle Wright-Babb, Committee Chairperson, Management Faculty
Dr. Johnny Morris, Committee Member, Management Faculty
Dr. Karina Kasztelnik, University Reviewer, Management Faculty

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

Walden University
2021

Abstract

Mitigating IT Security Risk in United States Healthcare:

A Qualitative Examination of Best Practices

by

JoAnn Hemann

Dissertation Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Philosophy

Management

Walden University

November 2021

Abstract

Cyberattacks are ranked as third in the top 10 highest global threats in terms of likelihood, ranked after extreme weather events and natural disasters. Traditional technology risk management plans for preventative, detective, and recovery measures have failed to mitigate cybersecurity risks created by new technologies. The social problem addressed was the impact of cybercrime to the healthcare industry. The purpose of this qualitative classical Delphi study was to determine how a panel of 25 healthcare cybersecurity experts, based in the United States, viewed the desirability, feasibility, and importance of information technology (IT) cybersecurity risk mitigation techniques. The conceptual framework selected for this qualitative study was the experiential learning theory. The basis of this theory was that we create knowledge via the transformation of our experiences. The literature provided proposed strategies to mitigate cybersecurity risk but was lacking in agreement on which methods are the most desirable, feasible, and important in reducing the risk of cyberattacks. Data were collected and analyzed during three rounds of iterative surveys to identify mitigation strategies based on the survey responses from chief information security officer cybersecurity experts. The top three strategies identified were establishing a cybersecurity program, implementing strong passwords and multifactor authentication, and cybersecurity hygiene. With this new knowledge, the healthcare industry cybersecurity professionals can better protect patient data enabling underserved communities to access healthcare in secure ways.

Mitigating IT Security Risk in United States Healthcare:

A Qualitative Examination of Best Practices

by

JoAnn Hemann

Dissertation Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Philosophy

Management

Walden University

November 2021

Dedication

This work is dedicated to my mom, Maureen Hemann, who has always been a great teacher and has kept a sense of humor even in tough times. She provided me with the motivation to keep learning, to stay focused, and enabled me to become the person I am today.

Acknowledgments

I would like to thank my parents, Robert and Maureen Hemann, who taught me the importance of a good education, to work hard, and to always do the right thing. Also, I would like to thank my children, Paul and Rachel, who know how long and hard this journey has been and have always been there when I needed motivation to keep going. I would like to also thank the academic leadership of Walden University. Specifically, I would like to thank my committee members, Drs. Danielle Wright-Babb, Johnny Morris, and Karina Kasztelnik, whose expertise, guidance, and support were instrumental during this process.

Table of Contents

List of Tables

List of Figures

Chapter 1: Introduction to the Study

The focus of this research was to identify cybersecurity strategies that will reduce the number of successful cyberattacks on the U.S. healthcare industry. Over the years from 2014 to 2019, cyberattacks on healthcare companies increased by 125% (Abraham et al., 2019). Based on these increasing attacks, cybersecurity in healthcare is an area of needed study. I aimed to fill the gap in the literature by identifying the most desirable, feasible, and important methods to reduce information technology (IT) threats and vulnerabilities in the U.S. healthcare industry.

In this study, I collected the perspectives and insights from U.S. healthcare chief information security officer (CISO) cybersecurity experts on which strategies are most desirable, feasible, and important. In 2018, it was found that 51.2% of the world's population used the internet, and by 2023 internet usage is expected to rise to 70% of the global population (Vakulyk et al., 2020). A recent example of how internet growth has improved healthcare access is surging telehealth capabilities. With the stay-at-home orders due to the global COVID-19 pandemic, telehealth has seen tremendous growth (Pointer, 2020). Telehealth has allowed the ability to receive healthcare without in-person appointments, thereby reducing the risk of infections (Wosik et al., 2020). With this technology growth, the risk of exposing personal data electronically has also risen, creating a lucrative opportunity for cybercriminals (Pointer, 2020). The expansion of the population using technology and rapid growth in such capabilities demonstrates the need to further study cybersecurity strategies to find ways to protect the growing number of technology users.

Potential social implications included an increased ability to provide medical care to underserved communities in a more safe and secure environment where personal health information (PHI) is appropriately protected. Implementing effective controls and remediating security gaps to reduce the effects of cyberattacks could improve the reputations of healthcare companies. This reputational improvement, coupled with the recent technology improvements (e.g., telemedicine), could enable an increased level of trust that PHI is properly protected, thereby increasing usage by populations with limited medical care.

This first chapter includes an introduction and a background of the study, describing the need for a better understanding of U.S. healthcare cybersecurity techniques. The following topics are included: problem statement, purpose of the study, research question, conceptual framework, and the nature of the study. Additional areas covered in Chapter 1 include definitions, assumptions, scope, delimitations, significance of the study, a summary, and the transition to the literature review in Chapter 2.

Background

Literature reviewed in preparation for this research study included the history of healthcare IT and technology advancements, which have created new problems in securing the PHI of patients. Traditional technology risk management plans for preventative, detective, and recovery measures have failed to mitigate cybersecurity risks created by these new technologies (Öbrand et al., 2018). The evolution of electronic health records (EHRs) and interconnected devices have been identified as one of the biggest contributors to the increase in cybercrimes related to healthcare (Coventry &

Branley, 2018). In addition to the creation of large data repositories of health information, the EHRs have increased accessibility to massive amounts of sensitive data—not only for healthcare providers, but also for cybercriminals (Ahmed et al., 2019; Hoffman, 2020). The growth of new IT areas such as the Cloud, Internet of Things (IoT), Bring Your Own Device (BYOD), Artificial Intelligence (AI), Shadow IT, and other technologies have added layers of complexity to cybersecurity (Atluri, 2018).

Federal regulations, frameworks, standards, and methodologies, such as the Health Information Portability and Accountability Act (HIPAA), the National Institute of Standards and Technology (NIST) Special Publications, and the Payment Card Industry Data Security Standard (PCI DSS), provide sets of rules, regulations, and guidance in protecting systems containing sensitive data (Schmeelk, 2020). Methods and terms for measuring and controlling the risk associated with cybersecurity programs have not been standardized (Radziwill & Benton, 2017; Schmeelk, 2020). There are similarities across these various standards; unfortunately, the differences are greater than the similarities.

One important domain included in the IT security frameworks is access control, which ensures the right permissions are assigned to users within IT systems, and that no more access than what is required is granted to each account (Azeez & der Vyver, 2019; Kaušpadienė et al., 2019). The implementation of these requirements is left to the healthcare organization and, in some cases, the requirements are intentionally vague so that they can apply to the large, medium, and small organizations that are implementing the controls.

The subjectivity of specific aspects of the requirements is also an issue. For example, the HIPAA security rule regulations are open to interpretation and are difficult to enforce due to terms such as *reasonable* (Cronin, 2020). In some organizations, after enterprise-wide risks are identified, they are risk ranked using the variables of impact and probability. Commonly assigned values are used to indicate the level of risk (e.g., low, medium, and high). Unfortunately, little guidance is provided to help determine which level should be assigned to each variable and result in risk rankings that are nonstandard across the industry. Standardization across risk management efforts should eventually help reduce confusion (Schmeelk (2020).

Cybersecurity attacks continue to increase, and there has been a significant increase in ransomware attacks against the healthcare industry (Hoffman, 2020; Morgan et al., 2020). Paying large amounts of ransom to unencrypt healthcare data and applications has caused financial and reputational damage (Morgan et al., 2020). The estimated cost of a single healthcare data breach is $2.2 million (Lee et al., 2018). Anderson (2018) indicated healthcare cyberattacks cost the industry $6.2 billion annually and globally cybercrime is predicted to cost $10.5 trillion by 2025, up from $3 trillion in 2015 (Cybersecurity Ventures, 2020). The financial positions and reputations of healthcare organizations are negatively impacted when cyberattacks are successful.

Cybersecurity mitigation methods were identified in the literature, and the gap in the research literature was that there is no consensus providing the most desirable, feasible, and important techniques for cybersecurity mitigation. This research was needed to provide an agreed-upon list of strategies and techniques that are thought to be the most desirable, feasible, and important in reducing the risk of being hacked, regardless of the technologies being used by U.S.-based healthcare companies.

Technology has transformed the way healthcare business is conducted and has provided new opportunities for cybercriminals. The two problems studied in this research included: (a) cyberattacks are ranked third in the list of global threats, and (b) traditional technology risk management plans have failed to mitigate cybersecurity risks created by new technologies. The literature reviewed on these two problems is summarized in the following two paragraphs.

Global Threat

Research literature indicated cybercrime is a worldwide problem (Ponemon Institute, 2018). Cyberattacks are ranked as third in the top 10 highest global threats in terms of likelihood (Cybersecurity Market Report, 2018). Healthcare companies are specifically targeted internationally by bad actors for three reasons:

1. The healthcare industry lags other leading industries in securing vital data and is a prime target for theft (Kruse et al., 2017).
2. Evolving medical technologies and threats require healthcare organizations to continue to adapt (Langer, 2017).
3. Medical records are more lucrative on the dark Web making them more attractive to the hackers because medical records can be sold for up to $1,000 each, which is 10 times more than credit card records since there is more personal information contained in health records (Pointer, 2020).

The issue of cyberattacks on healthcare is a global issue; however, I focused this research on large U.S.-based healthcare companies providing medical care in the United States. Additional work in this area of study could easily be extended to other worldwide industries that utilize IT.

Mitigation

The literature on the topic of cybersecurity related to risk mitigation confirms there is no standardized approach for deterring cybercrime. Healthcare organizations continue to see large increases in cybercrimes (Abraham et al., 2019). Despite federal regulations aimed at protecting PHI (i.e., HIPAA) and the General Data Protection Regulation (GDPR) in Europe, many healthcare organizations have not implemented what is required to protect PHI. There is a balance between cybersecurity measures and the usability of healthcare systems that support patient care that must be determined (Dameff et al., 2019). This balance varies depending on the risk appetite of the healthcare organization and its cybersecurity culture and posture.

This research was needed as there is a gap in the literature showing a consensus of the most desirable, feasible, and important strategies U.S.-based healthcare companies should have in place to mitigate the risk of cyberattacks. This was the identified gap into which I intended to provide insight by identifying the most desirable, feasible, and important methods to avoid a breach. The review of the literature provided the ability to gain an extensive background of cybersecurity and support the problem statement identified.

Problem Statement

Over the years from 2014 to 2019, cyberattacks on healthcare companies increased by 125% (Abraham et al., 2019). Not all healthcare information technology (HIT) organizations have implemented comprehensive robust security plans that address preventative, detective, and recovery measures (Abraham et al., 2019). The costs associated with healthcare breaches also continue to rise. According to PR Newswire (2019), “The estimated cost of a data breach by the respondent hospital organizations with actual breaches in 2019 averaged $423 per record” (para. 11). This is up from the previously reported $408 per record in 2018, which was more than double that of other industry breaches (e.g., financial and services; Ponemon Institute, 2018).

The general management problem is that cyberattacks are ranked as third in the top 10 highest global threats in terms of likelihood, ranked after extreme weather events and natural disasters. It has been estimated that by 2021 cybercrime will cost the world $6 trillion annually (Cybersecurity Market Report, 2018). The social problem addressed is the impact of cybercrime on the U.S.-based healthcare industry (Lee et al., 2018).

The specific management problem is that traditional technology risk management plans for preventative, detective, and recovery measures have failed to mitigate cybersecurity risks created by new technologies in healthcare (Öbrand et al., 2018). The healthcare industry lags behind other leading industries in securing vital data and, as a result, healthcare organizations have become a prime target for theft (Kruse et al., 2017).

Purpose of the Study

The purpose of this qualitative classical Delphi study was to determine how a panel of 25 U.S.-based healthcare CISO cybersecurity experts views the desirability, feasibility, and importance of IT cybersecurity risk mitigation techniques. Relying on subject matter experts to provide opinions on the most effective mitigation techniques and how to keep up with the evolving threats, the hope was to leverage the years of knowledge and perspectives from practitioners to share what they have learned. The information gained can then be utilized by other healthcare CISOs to help determine the path forward for the implementation of effective cybersecurity risk mitigation techniques.

Research Question

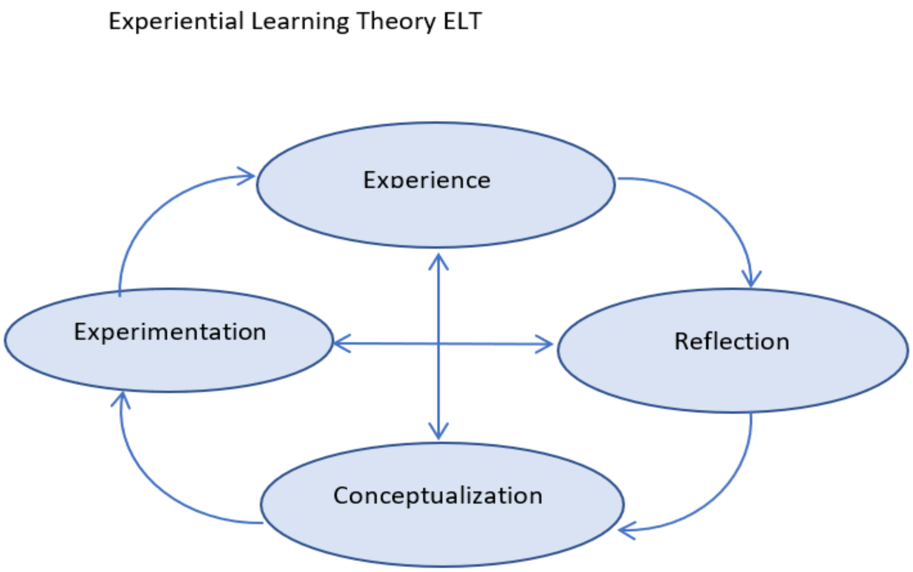
The following research question guided this qualitative classical Delphi study: What are the U.S. IT healthcare cybersecurity experts' views on the desirability, feasibility, and importance of effective cybersecurity risk mitigation techniques? This research question relied on experiences of the experts to determine the level of consensus on risk mitigation techniques.

Conceptual Framework

The conceptual framework selected for this qualitative classical Delphi study was the experiential learning theory (ELT; Kolb & Kolb, 2009). The basis of the ELT is that knowledge is created via the transformation of our experiences. The diagram in Figure 1 depicts this learning cycle showing the iterative process of experiencing, reflecting, conceptualizing, and experimenting.

Figure 1

Experiential Learning Theory



Note. Adapted from “Experiential Learning Theory: A Dynamic, Holistic Approach to Management Learning, Education and Development,” by A. Kolb and D. Kolb, in S. J. Armstrong and C. V. Fukami (Eds.), *The SAGE Handbook of Management Learning, Education and Development*, 2009, Sage (https://doi.org/10.4135/9780857021038.n3).

For this research study, the intent was to gain knowledge through the lens of individuals with extensive years of experience in combatting cyberattacks. CISOs in large U.S.-based healthcare organizations provided their unique insights and perspectives. I provided the ability to share that knowledge in the CISOs’ own organizations and externally to other IT organizations to improve cybersecurity practices across the industry.

A more thorough examination of cybersecurity topics such as why healthcare is targeted by cybercriminals and the various types of common attacks will be provided in the literature review in Chapter 2. The participants in the study relied on their unique experiences and perspectives to provide information on what has worked and what has not worked in their specific organization. Practitioners confirmed through their experience, reflection, thoughts, and actions that the steps they have already taken and proven to reduce risk are effective. In addition, the strategies that are not effective will be identified. It was understood that the ineffective strategies were less likely to be shared by the participants.

Nature of the Study

A qualitative classical Delphi methodology was used to identify effective risk mitigation methods among healthcare cybersecurity experts for IT cybersecurity risk in large U.S.-based healthcare organizations with annual revenues over $50 million. A qualitative methodology was an appropriate choice as the experiences of experts were gathered via iterative surveys to determine the optimal ways to mitigate risk. Quantitative and mixed methods attempt to prove hypotheses, which was not my goal in this research. The Delphi method is flexible and affordable and was a good fit for this type of study to gain experts' consensus (Brady, 2016).

The qualitative classical Delphi study population included IT cybersecurity experts in large U.S.-based healthcare organizations who had a minimum of at least 10 years of experience. Initially, 25 subjects were selected to answer open-ended iterative electronic survey questions. The subjects were requested from various IT Healthcare

LinkedIn groups and the snowball technique was used to identify additional subjects. Also, SurveyMonkey (https://www.surveymonkey.com/) had an option to identify participants for the study; however, there was a high cost associated with this method and it was not used. Additional participants were recruited by searching for contact information on the internet.

The iterative surveys were completed online using SurveyMonkey—a free internet-based survey tool. The intent was to gather information on the most desirable, feasible, and important mitigation techniques from experienced IT security and risk management professionals in large U.S.-based healthcare organizations. The first step was to conduct the initial survey and gather data about the perceptions of risk mitigation techniques. The data gathered were utilized for additional survey questions. A series of three survey rounds to gather information was used to identify the top three most frequently occurring mitigation methods.

Data gathered from each round of survey iterations were analyzed using Microsoft Excel, then coded, and the results were utilized to drive additional more detailed questions. The data drove the direction for subsequent iterations to further refine results and gain consensus from the study participants. Using data analysis tools that are well suited for qualitative studies assisted in attaining results from each of the iterations in a timely manner. In addition, the analyses tools helped ensure data were trustworthy, and data triangulation was used to ensure data were valid.

Possible Types and Sources of Data

Sources of information included the following:

1. Survey responses from multiple iterations of surveys from 25 participants who met the following inclusion criteria:
    - Cybersecurity subject matter experts;
    - A minimum of at least 10 years of IT security experience at large U.S.-based healthcare companies; and
    - Expertise in risk mitigation and cybersecurity framework implementation.
2. Previously published research articles, literature, and case studies.
3. Reflexive journal notes from throughout the study.
4. Related Walden University dissertation by Barosy (2019), *Successful Operational Cybersecurity Strategies for Small Businesses*.
5. Related Walden University dissertation by Cook (2017), *Effective Cybersecurity Strategies for Small Businesses*.
6. Related dissertation by Gibson (2020), *A Comprehensive Strategy for Cybersecurity Implementation Within the Department of Defense: A Delphi Study*.

Definitions

Chief information security officer (CISO): C-suite level employee who is responsible for the establishment of the organizational security strategy and ensures that all data assets are inventoried and protected (Samuels, 2020).

Cybersecurity: Steps that will help to prevent the damage of computer systems, enable the protection and restoration of computer systems (including information contained to ensure the availability, integrity, authentication, and confidentiality; NIST, 2020). Traditional information security has focused on the protection of IT sources and the roles of humans in the security processes, whereas cybersecurity also includes humans as potential targets of cyberattacks or participants in a cyberattack (Aaltola & Taitto, 2019).

Detective measures: Used by a company to identify nefarious or irregular activities so they can be investigated and corrected as promptly as possible to avoid additional damages (McMahon, 2020).

ePHI: Electronic protected health information is defined as any PHI that is created, stored, transmitted, or received in any electronic format or media. There are 18 data fields considered as ePHI (Compliancy Group, 2020).

HIPAA: The Health Insurance Portability and Accountability Act of 1996 required the Secretary of the U.S. Department of Health and Human Services (HHS) to develop regulations protecting the privacy and security of certain health information. To fulfill this requirement, HHS published what is commonly known as the HIPAA privacy rule and the HIPAA security rule (HHS, Office of Civil Rights, 2020).

Meaningful Use (MU): A government-driven directive that seeks to encourage the use of EHRs by medical professionals and health information industries. The program is intended to move the healthcare industry away from a paper-based system and toward a digital network for greater efficiency (Bullard, 2020).

Phishing: The practice of sending emails claiming a false identity to induce users to reveal information (Jalali et al., 2020).

Preventative measures: An organization performs these activities to make it more difficult for an attacker to compromise its systems, including vulnerability testing and server hardening, network segmentation, password hygiene, and user access provisioning controls (Bakertilly, 2016).

Privacy rule: The HIPAA privacy rule establishes national standards for the protection of certain health information (HHS, Office of Civil Rights, 2020).

Recovery measures: After a breach or other incident has occurred, action must be taken to returns systems to normal activity. This includes the creation of an incident response plan, which is a communication plan, an approach to restore affected services, documenting the root cause of the incident, and the implementation changes to remediate the risk of the same type of incident happening again (Bakertilly, 2016).

Security rule: The HIPAA security rule establishes a national set of security standards for protecting certain health information that is held or transferred in electronic form (HHS, Office of Civil Rights, 2013).

Threat: Event or condition with the potential to adversely impact organizational operations, assets, or users via unauthorized access, destruction, disclosure, modification of information and/or denial of service (Joint Task Force Transformation Initiative, 2015).

Vulnerability: Weakness in an information system that could be exploited by a threat source (Joint Task Force Transformation Initiative, 2015).

Assumptions

To improve data quality, a few aspects that cannot be proven true are identified. One assumption was that there was an ability to gain agreement from the CISOs on the most effective measures to combat cyberterrorism. Another assumption was that the survey respondents will understand the questions and answer truthfully, relying on their lived experiences. The participants met the criteria established so they could rely on the experience and knowledge gained over the years. The participants engaged in this study have volunteered and have an interest in the results of the study. It was assumed that they answered the survey honestly and to the best of their abilities to ensure the best outcome. Also, in the survey directions, it was stressed that the respondents understand the importance of each answer being as truthful as possible. These additional steps helped to improve the quality of responses.

Scope and Delimitations

The scope for this research was limited to gathering cybersecurity information on strategies implemented by large U.S.-based healthcare company CISOs to determine what methods they find most desirable, feasible, and important. Delimitations are decisions the researcher has made regarding boundaries of the study and can control but has decided not to include them in the study (Creswell & Creswell, 2018). The scope and delimitations were selected because there continues to be an increase in cyberattacks that specifically target healthcare data.

There was no consideration of participants based on race, gender, or age because the diversity of the CISOs is not relevant in this study. The participants are limited to

U.S.-based cybersecurity experts who have a direct influence in setting the direction for strategies to protect ePHI in their organizations. Language barriers were eliminated by limiting to U.S.-based CISOs, which is important in a survey-based study.

The experiences of the CISOs vary. Therefore, the study was limited to those who have held the position for a minimum of at least 10 years. This timeframe was selected as newly appointed CISOs may not have the knowledge to adequately indicate which strategies are desirable, feasible, or important. Some organizations experience fewer cyberattacks than others, and the goal of the study was to determine what those organizations are doing that keeps them from being attacked; however, there was no delimitation based on the number of past breaches. Requiring an organization to reveal past breaches would not be conducive to the study. The results of this research will transfer to other organizations that rely heavily on IT and are targeted by cybercriminals. The results are transferable to organizations outside of the U.S. healthcare industry and can potentially apply to large and small organizations.

Limitations

One limitation was analyzing the results of this qualitative classical Delphi study as there was little guidance in the literature on the process of thematic analysis. Additionally, the generalization of the results to a wider population regarding sample size, geographical location, or limited views might not be possible. The opinions of a small group of cybersecurity experts might not hold if additional work is completed with a wider scope. To address this need, it is recommended that additional studies be done to validate the findings with a larger number of participants in a different country or a different industry.

Another limitation was that the questions were delivered via an electronic survey to security experts in U.S.-based healthcare organizations. Nonverbal and non-face-to-face communication could have been difficult; however, the survey questions were well written and thought out. One challenge for me, because I have worked in the IT field for over 30 years, was keeping personal bias in check. My experiences and background had the potential to drive me to ask questions in ways to find the answers that were already decided in my opinion. The experts provided their perspective, which I was able to manage, without judging whether they were right or not.

A barrier considered was the physical distance between the survey participants. There were no follow-up questions needing to be answered from the participants; however, if needed these were planned to be handled via telephone or web conferencing meetings, as there was to be no face-to-face contact during the study. This barrier did not degrade communication as body language and facial expressions of the subjects were unseen. The ability to use collaboration tools such as Zoom, Microsoft Teams, Webex, and other video communication tools could have helped remove this barrier.

Significance of the Study

The significance of this research was that it could identify the most effective risk mitigation techniques based on expert opinions of subject matter experts. The results can be utilized by healthcare organizations and other industries to reduce the levels of IT cybersecurity risk and increase protection against hackers. This research could result in a new theory or framework, improve the way risk is managed in healthcare organizations, and increase the level of patient trust that their PHI is sufficiently being protected. The positive social change was that underserved populations could have increased access to medical care through new technology that is secure and safe for use.

Significance to Theory

This research attempted to advance understanding of the most effective strategies by identifying best practices for mitigation of cybersecurity risks. Organizations could be better positioned to keep their data secure by implementing the strategies to reduce risk. The existing standards and frameworks help organizations become compliant with the regulations, but compliance does not necessarily equate to secure systems. These frameworks are overly burdensome and difficult to understand. “The preponderance of healthcare-related laws, compliance regulations, and security guidance frameworks serve to complicate the cybersecurity challenge further and too often results in senior leadership assuming a state of blissful ignorance” (Abraham et al., 2019, p. 1).

Significance to Practice

All IT industries could benefit from research on this topic as it could help organizations identify effective methods of securing various types of confidential and sensitive data (Henriques de Gusmão et al., 2018). Within the healthcare industry, securing patient data continues to be top priority for leadership (Peterson et al., 2018). Finding the most effective mitigation techniques and ensuring proper prioritization of efforts are critical to keeping the trust of the patients. These mitigation techniques can be applied beyond healthcare in other IT industries.

Significance to Social Change

Positive social change implications included increasing the accessibility of healthcare using technology in a secure and safe manner. Reducing the number of healthcare cybercrime attacks will potentially reduce the cost incurred by the healthcare organization and will increase patients trust factors. With stolen identity occurrences, the patients may lose trust in the healthcare organization. According to Lee et al. (2018), the cost estimate of a healthcare data breach is $2.2 million. Implementing strong mitigation mechanisms to keep a breach from happening will pay for itself (Hausfeld & Zimmerman, 2018). An increased level of patient trust could help healthcare organizations reach areas of underserved populations.

Summary and Transition

This chapter included an introduction to the research topic and provided a detailed background showing the need for a better understanding of healthcare cybersecurity techniques. The following topics are also included: problem statement, purpose of the study, research question, conceptual framework, and the nature of the study. The additional areas include definitions, assumptions, scope, delimitations, significance of the study, summary, and the transition to the literature review in Chapter 2.

The literature review in Chapter 2 begins with a broad healthcare technology background and the impacts on advancements in technology. Sharing healthcare data in an electronic medical record (EMR) method has had positive and negative impacts. Frameworks have been developed to secure data but are largely unsuccessful in stopping cybercriminals from hacking into the systems. Healthcare data is targeted because it is more lucrative than other industry data. Types of attacks and costs involved are discussed, and a list of mitigation strategies concludes Chapter 2.

Chapter 2: Literature Review

The general management problem was that cyberattacks were ranked as third in the top 10 highest global threats in terms of likelihood after extreme weather events and natural disasters (Cybersecurity Market Report, 2018). The specific management problem was that traditional technology risk management plans for preventative, detective, and recovery measures have failed to mitigate cybersecurity risks created by new technologies in healthcare (Öbrand et al., 2018). The purpose of this qualitative classical Delphi study was to determine how a panel of 25 CISOs in U.S.-based healthcare organizations views the desirability, feasibility, and importance of IT cybersecurity risk mitigation techniques.

The literature indicated that the growth of cyberattacks against healthcare companies is due to technology advances and a lack of successful mitigation strategies. The hackers are targeting medical record data as they are much more lucrative than other forms of information. Hackers are staying a step ahead of the cybersecurity professionals and continuously creating new ways to attack. Defending against hackers is costly. Adding to the cost includes ransom and fines paid to the federal government for noncompliance with regulations that protect health information. There is no single solution to keep sensitive data protected—a layered approach is recommended (Connolly & Wall, 2019). Mitigation strategies vary by industry, and there is no standardized set of strategies identified that will protect against threats and vulnerabilities.

The major sections of the literature review include the background of IT in healthcare and the impacts of technology advancements, sharing healthcare data through

EHRs, frameworks and methodologies to secure data, reasons hackers target healthcare technology, types of cyberattacks, costs involved, mitigation strategies, and concludes with a summary of the chapter.

Literature Search Strategy

Searching for relevant and recent peer-reviewed articles on this topic was difficult as cybersecurity is a relatively new and not a strong academic topic. In searching for relative articles, I used primarily the Walden Library search engine, which allowed access to the EBSCO, ProQuest, ResearchGate, and ScienceDirect articles. Google Scholar was also used when sufficient articles were difficult to find. Time frames for published dates were limited to 2017–2021 and the *peer-reviewed only* checkbox was selected. Search terms included: *cybersecurity* AND *healthcare, history of IT, digitization of healthcare, healthcare data, breach, cyber strategies, hackers* AND *healthcare, types of cyberattacks, cyber costs, cyber mitigation, strategies to mitigate cyber risk, meaningful use, Health Information Technology for Economic and Clinical Health (HITECH), Health Insurance Portability and Accountability Act (HIPAA), Sarbanes-Oxley Act (SOX), Payment Card Industry Data Security Standard (PCI DSS), Qualified Security Assessor (QSA), ransomware,* and *malware.* In many cases, iterations of searching for various terms were required to reduce the number of articles returned. More specific terms helped to limit the articles to those most relevant.

Conceptual Framework

The conceptual framework selected for this qualitative classical Delphi study was the ELT (Kolb & Kolb, 2009). The basis of the ELT is that knowledge is created via the transformation of our experiences, as previously discussed in Chapter 1. The learning cycle is an iterative process of experiencing, reflecting, conceptualizing, and experimenting. The knowledge gained for this study was gathered from CISO cybersecurity experts who work in a U.S.-based healthcare organization, relying on their unique experience and perspectives to provide information on what has worked and what has not worked in their organizations. Practitioners confirmed through their experience, reflection, thoughts, and actions that the steps they have already taken and were proven to reduce risk, were effective. The hope was to gain the knowledge to identify the most desirable, feasible, and important mitigation techniques.

Literature Review

Background and Impact—HIT

The background and impact of technology growth on healthcare are discussed in this section. Since the 1960s, advancements in HIT continue to have a positive effect on health (Kruse & Beane, 2018). Yan et al. (2018) indicated that 55% of the studies reviewed showed positive effects of HIT in areas such as timeliness and effectiveness, provider and patient adherence, and perceived care quality. There was also evidence in the literature that HIT contributed to the increased life expectancy rates.

These advancements, however, have had the negative impact of opening the door to increased cybercrime targeting lucrative healthcare data (Ibarra et al., 2019). With additional evolution, federal government incentives, and requirements for the EHR, sensitive medical data was gathered and stored electronically, which enabled that data to be easily shared. This section also provides the advantages and disadvantages of EHRs, and then more narrowly reviews a brief history software development methodology.

Improvements in HIT have increased life expectancy (Negash et al., 2018). According to DeWitt (2018), 100 years ago, the life expectancy was 39; however, after the Spanish Flu pandemic, the life expectancy dramatically increased to 55. In comparison to more recent years, the average life expectancy in the U.S. for 2020 is 77.8 years (Burdorf, et al., 2021). This is more than double the pre-Spanish Flu numbers. Many things have evolved over the past 100 years, and several reasons are contributing to why we are living longer. Technology advancements in healthcare are arguably one of the major drivers. "Over the past few decades, we have witnessed a dramatic rise in life expectancy owing to significant advances in medical science and technology, medicine as well as increased awareness about nutrition, education, and environmental and personal hygiene" (Sumit & Deen, 2019, p. 1).

Healthcare technology is providing options for delivery of healthcare previously not available. Tyson (2017) indicated that 52% of healthcare encounters with primary care physicians are done virtually. To further support Tyson on virtual care, with the response to COVID-19, the explosive growth of telehealth has allowed for medical care to take place virtually without risk of face-to-face transmission (Wosik et al., 2020). Schroeder (2019) indicated telehealth as an opportunity, "From infusion pumps to eICUs to home management technology to telehealth, there's tremendous opportunity to improve access to and quality of care" (p. 25). Technology continues to change the way healthcare is delivered and has improved access to and quality of healthcare.

A brief review of the history of technology is helpful for understanding how the evolution of this technology has created the problem of securing healthcare data to avoid breaches. According to Yun et al. (2019), through the mid-1980s, mainframe computers were used to process high volumes of data with centralized computing power, resulting in the ability to collect data; however, analyzing the data and search engines had not progressed enough to provide meaningful usage of the collected data. During the mid-1990s the internet began to influence the way businesses, consumers, government, and media communicated, and during the early 2000s the social media age emerged (Yun et al.). The ability to connect to the internet and share information socially enabled unpredicted growth, which contributed to the sharing of PHI.

Enabling Sharing of Healthcare Data

With the expansion of information systems in the industry, EMR and EHR systems were developed to store information about patients without using paper-based medical records to facilitate data collection and demonstrate quality improvements (Schroeder, 2019). EMR and EHR are quite similar and are often used interchangeably, which is incorrect. The differences are pointed out by Stacy (2019):

> Occasionally, the term *electronic medical record* (EMR) is used interchangeably (but incorrectly) with EHR. An EMR is usually created in one place (a clinic, doctor’s office, or hospital) and only focuses on a specific problem and its treatment. EHRs have become a preferred means of recording information because of the ease with which they can be sent from one facility to another as well as their ability to easily contain information from different sources. (p. 1)

For this dissertation, I used the term EHR rather than EMR based on Stacy's explanation.

The federal government enticed healthcare companies to rapidly move to EHR systems with the meaningful use program. According to Sorace et al. (2020),

> The Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 authorized the Centers for Medicare and Medicaid Services (CMS) to provide incentive payments to healthcare providers if they adopt and meaningfully use (MU) electronic health records (EHRs). As of 2016, CMS spent over $34 billion in incentive payments (p. 1).

As a result, the adoption rates by healthcare organizations to use the EHRs are high; however, it was met with resistance from physicians and nurses who felt there were higher priorities in the healthcare organizations. While increasing the ability to provide improved medical care, the personal data of millions of U.S. citizens had become electronically available and targeted for cyberattacks. The following two sections outline the advantages and disadvantages of migrating to EHRs.

Advantages of EHRs

There are many benefits to using EHRs. Positive consequences of the EHR implementation include the emergence of massive quantities of health-related data and this EHR data is tremendously improving the quality of healthcare services provided (Techapanupreed & Kurutach, 2020). Medical information is easy to share when using EHRs, and patient information can be accessed and updated as treatment is provided (Keshta & Odeh, 2020). Kopel et al. (2019) indicated that the advantages of EHRs include the ability to organize data to improve patient care and enable the ability to track the practice data to compare with national standards. Also, the EHR helps with research efforts and prescribing electronically has prevented errors related to drug interactions and allergies. "An effective EHR trends clinical conditions and responses; tracks clinical interventions; integrates data, such as lab results, with medication management; and triggers high-risk situations—all central to ensuring high-quality, safe care" (Schroeder, 2019, p. 24).

Bajric (2020) summarized the advantages of EHRs to include the following:

- time is saved by physicians in documenting patient visits;
- quality of healthcare provided is improved and medical errors are reduced;
- patient travel time to in-office visits is reduced;
- there are no paper copies of the medical record that can be misplaced or stolen;
- some physician handwriting is illegible; and
- physician and patient have access to view information live anytime.

However, contradicting Bajric about time being saved, Schroeder (2019) indicated that the time for physicians to document is taking much longer with the EHR systems, with some reports of over 50% of work time being taken away from patient care.

Summarizing the literature on the topic of the benefits of EHRs, the authors of literature indicated that:

- Health information can be easily viewed, updated, shared, and organized (Bajric, 2020; Keshta & Odeh, 2020; Kopel et al., 2019).
- Comparisons with national standards can be made (Kopel et al., 2019).

- Research efforts are improved with quality data (Kopel et al., 2019).
- E-prescription errors can be reduced (Kopel et al., 2019).
- Physician time is saved to document patient information (Bajric).
- Travel time is reduced for patients and physicians (Bajric).

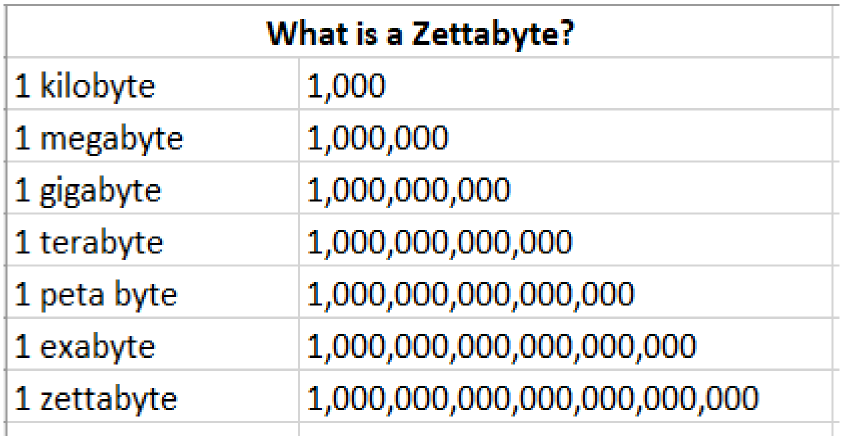
The move to EHRs has had a positive impact on healthcare. In the relatively short amount of time that EHRs have been in use, many new benefits have been realized. There are many disadvantages, though, which arguably may lead people to think paper records might have been better.

Disadvantages of EHR

Researchers have described a number of negative aspects of collecting protected health information within EHRs. According to Akhtar et al. (2020) “A tremendous amount of data is being produced at an alarming rate in all medical data centers. The volume of data is predicted to reach 35 zettabytes by 2020” (p. 61). A zettabyte is such a large number, conceptualizing how much data a zettabyte contains is difficult. Figure 2 facilitates putting the size of a zettabyte into perspective.

Figure 2

What is a Zettabyte?



What is a Zettabyte?	
1 kilobyte	1,000
1 megabyte	1,000,000
1 gigabyte	1,000,000,000
1 terabyte	1,000,000,000,000
1 peta byte	1,000,000,000,000,000
1 exabyte	1,000,000,000,000,000,000
1 zettabyte	1,000,000,000,000,000,000,000

Note. Adapted from "The Impact of Big Data in Healthcare Analytics." By U. Akhtar, J.W. Lee, H. S. Muhammad Bilal, T. Ali, W. A. Khan, & S. Lee, 2020, *International Conference on Information Networking (ICOIN)*, p. 61. (https://doi.org/10.1109/ICOIN48656.2020.9016588).

Large quantities of personal medical data have been collected and will continue to be collected considering the growth in technology (e.g., health monitoring using mobile technology; Meng et al., 2018). This large quantity of ePHI is increasingly being targeted by cybercriminals because of the data it includes (e.g., patient name, address, social security number, medical record number, and phone number; Tao et al., 2019). There are 18 fields defined by the federal government as ePHI that must be protected according to federal law; these 18 fields enable unique identification of the patient (Compliancy Group, 2020).

Another disadvantage in implementing EHRs came with the urgency to receive financial incentives for meaningful use and the increased priority and new systems were not always positively received by the medical community. This rapid adoption resulted in unintended consequences and the original intent to lower the costs of healthcare was not met. According to Colicchio et al. (2019), the EHRs implemented were ineffective and barely met the requirements of meaningful use; however, U.S. healthcare is still the most expensive and lags in quality outcomes when compared with other countries. This rapid move to EHRs and the lack of investment in cybersecurity has continued to leave the healthcare sector vulnerable to attack (Coventry & Branley, 2018).

Bajric (2020) pointed out that the disadvantages of EHRs include unauthorized access to patient files; the EHR application must be updated to reduce security vulnerabilities, and EHR systems are expensive. The most serious of the disadvantages is that massive quantities of ePHI data can be stolen quickly and the unauthorized access from hackers can go undetected for months, if not years (Botelho, 2017).

Disadvantages of implementation of EHRs as described in the literature include the following:

- Massive quantities of PHI are being collected (Akhtar et al., 2020; Meng et al., 2018).
- Hackers are increasingly targeting PHI (Tao et al., 2019).
- Rapid implementation of EHRs caused unintended consequences (Colicchio et al., 2019).
- Lack of investment in cybersecurity left data vulnerable (Coventry & Branley, 2018).
- Unauthorized access to patient files may be gained (Bajric, 2020).

- EHRs must be updated and are expensive (Bajric, 2020).
- Ability for hackers to steal millions of records very quickly is increased with large databases (Botelho, 2017).
- Undetected breaches for months and possibly years (Botelho, 2017).

This sharing of data would not have been possible without the EHR and the advances made in technology, including hardware (i.e., servers, laptops, mobile devices, etc.) and software, which are applications that run on the hardware. Software development processes improved rapidly, allowing for healthcare applications and databases to continue to improve and grow (Kalso, 2020).

Software Development Evolution

The rapid advances of technology have required software engineers to design software quickly and efficiently while ensuring improvements of its predecessors (Kalso, 2020). Royce (1987) outlined the waterfall model and indicated it was inefficient for software development. In the waterfall model, the software project is executed phase-by-phase. First, the requirements phase is completed, then the design phase, a development phase, and one testing phase. Each phase was completed before moving to the next, and one product was delivered to the client. Projects were consistently over budget, not on time, and did not meet the needs of their clients. Healthcare business clients were not impressed by the cost and length of time these products were taking to deliver.

In the last 20 years, improvements in software development allowed for faster cycle time and improved quality products to evolve (Gonen & Sawant, 2020). The iterative agile software development methodology was introduced in 2001, where smaller chunks of the project are rolled out, allowing clients to provide feedback much quicker. Daily scrum meetings drive the events in 15- to 30-day sprints, overall improving cycle time for project completion and increasing the likelihood of project success (Al-Saqqa et al., 2020). It is also being realized that security should be built into the software development process, beginning at the very first steps (Cope, 2020).

The continued growth of new technologies (e.g., the Cloud, IoT, BYOD, AI, Shadow IT) and other areas have added a layer of complexity to security (Atluri, 2018). Understanding the roles and responsibilities of implementation and support of these complex systems, and understanding who has ownership of the required security controls that protect the data while being stored, processed, and transmitted, is more complex when services are provided in these multi-layered environments. With these new technologies, the competition across IT firms providing services to healthcare companies continued to drive innovation and growth.

Competitiveness

The education of healthcare and IT professionals evolved dramatically during the digitization period as information provided to the physician and the patient becomes more accessible. Patients routinely search on Google to determine if their symptoms might be serious enough to make a doctor appointment or search to find the details on the latest home remedy. The race has begun for healthcare organizations to provide Web-enabled, easy-to-understand, correct information that the population can trust.

Competitiveness in the healthcare industry relied on continually driving IT advancements. To be more prepared for the global IT market in the future, Isabelle et al.

(2020) indicated that Porter's Five Forces Model can still be utilized and applied for IT competitive bargaining power. Porter's five forces are listed below with the IT perspective provided in the article:

1. Rivalry—the rise of digital technologies and e-business has increased rivalry among firms; companies no longer need to own their physical infrastructures and financial resources to invest/acquire innovative companies.
2. The Threat of Substitutes—international business is easier, substitute products can be digital or hybrid, switching costs are low and digital marketplaces have emerged.
3. Buyer Power—there are many IT firm options for consumers to choose from, easy access to information for buyers, and expectations for customer experiences is evolving which leads to high pressure for IT firms.
4. Supplier Power—the notion of suppliers is expanding as they can use high bargaining power to slow down disruptive models, suppliers can be government regulators supplying critical permits and licenses, finding and retaining IT employees is very difficult, data aggregators have bargaining power given their expertise.
5. The Threat of New Entrants—there are low barriers to entry, firms compete globally with no physical presence, digital-based business models are easily scalable and are much less capital intensive (Isabelle et al., 2020).

Advancements continue, in part, due to the fierce competition to get products to market in many healthcare areas (i.e., mobile, medical devices, telehealth, remote patient monitoring, wearables, robotic surgery, and artificial intelligence applications for diagnosing disease and finding cures). The public has been provided readily available tools and information with advice for diet, exercise, and mental health that will also drive healthier lifestyles and increase life expectancies. The focus of healthcare is moving toward healthier lifestyle choices and not getting sick to begin with. According to Tyson (2019), “America's healthcare system today is a ‘fix-me system’ in which patients seek hospital care when they are already ill. This approach is expensive and often too little too late in terms of medical interventions” (p. 1).

To summarize this section, the glimpse into the success of the past HIT and the emergence of sharing information, specifically within EHRs and the growth of massive amounts of data, there are many positive impacts for healthcare being realized. Software development and the competition continue to drive increased quality and speed in the implementation of the new technology. Staying competitive in the healthcare industry market is important and the ever-increasing demand for cybersecurity and HIT services outweighs the supply. Steps have been taken to combat the negative impacts of the growth in cybersecurity threats, but understanding why healthcare is targeted will provide insight on the proper steps to alleviate hackers being successful with their attacks. Cybercriminals are seizing this opportunity for financial gain and we are witnessing an unprecedented increase in attacks targeting healthcare data.

Why Is Healthcare Data Targeted by Hackers?

Technical and Financial Factors

There are technical and financial reasons why healthcare organizations are being targeted aggressively by hackers (Tao et al., 2019). According to Tao et al. (2019), the attack surfaces in healthcare organizations are large, and IT systems in healthcare are notorious for using outdated hardware and software that are more vulnerable to cyberattacks. Tao et al. indicated the main financial reason is that the patient data (e.g., name, address, phone, social security number, etc.) is 10 times more valuable per record than a credit card number. Tao et al. also indicated a credit card number can be sold on the black market for $3 to $5 per record, while the average amount for a medical record sold on the black market is $50. Pointer (2020) indicated some medical records sell for $1,000 each on the dark Web. It is not clear why there is such a difference in the reported amounts; however, additional research could be done to clarify.

The reason medical records are more valuable is that credit card companies are improving capabilities for fraud detection and will lock credit cards from additional charges if suspicious charges are being made. The cybercriminal can only use the card until it is maxed out, canceled, or locked. The personal data stolen from healthcare records allows hackers to create new credit accounts that could go undetected for months.

Abraham et al. (2019) indicated reasons for increased activity include the rapidly expanding attack surfaces along with sensitive and valuable data. These are making healthcare organizations more vulnerable to attack and they appeal to the hackers. Additionally, too many healthcare organizations have out-of-date systems (Branch et al., 2019). Kruse et al. (2017) concluded that the "healthcare industry is a prime target for medical information theft as it lags behind other leading industries in securing vital data" (p. 1). There is agreement from multiple authors on these technical and financial reasons for why healthcare organizations are targeted. Additional information in the following section further identifies issues in the systems of healthcare organizations.

Insecure Healthcare Systems

Emerging medical technologies and devices continue to be added into healthcare organization's IT networks expanding the attack surface (Atluri, 2018; Branch, 2019; Coventry & Branley, 2018). New medical and mobile devices that monitor patient information are connecting through the internet and are especially vulnerable to a broader range of cyber threats (Meng et al., 2018). These devices are not always thoroughly tested before being implemented and connected to the network, increasing the probability that sufficient cybersecurity measures were not put into place. Steps are being taken in various healthcare organizations to "elevate the importance of cybersecurity throughout the entire device life cycle, from the request to procure a device all the way through to decommissioning" (Stern, 2018, p. 465). Medical devices continue to increase the probability of a successful attack.

Vendor-provided IT services (e.g., Cloud and Environment-as-a-Service) are being utilized at a higher frequency due to cost savings. Atluri (2018) indicated that before and after migrating into the Cloud there are risks to be managed, and there should be clear roles and responsibilities when it comes to managing that risk. Technologies such as these are continuing to grow the attack surface where hackers can gain access to the network and the PHI data contained therein.

The costs to adequately protect information systems are high, and funds in healthcare organizations are not being appropriately allocated to protect the systems. Atluri (2018) indicated that 4 to 6 percent of the IT budget in healthcare systems is spent on cybersecurity. Considering the life-threatening capability of cyberattacks on medical devices (e.g., infusion pump, ventilators, scanners, implantable pacemakers, etc.), the priorities and financial allocations should be reprioritized in healthcare organizations (Branch, 2019). “It is imperative that time and funding is invested in maintaining and ensuring the protection of healthcare technology and the confidentially of patient information from unauthorized access” (Kruse et al., 2017, p. 1).

To add to the cost of securing systems, well-trained cybersecurity staff is scarce and expensive. Coventry and Branley (2018) indicated that there is a lack of cybersecurity expertise in the healthcare sector. According to Castro (2018), in March 2018 there were 285,000 cybersecurity job openings in the U.S. The International Information System Security Certification Consortium (as cited in Castro, 2018) estimated that by the year 2022, there is an expected global shortage of 1.8 million cybersecurity workers.

Turnover rates are high in the cybersecurity workforce, only 15 percent of cyberprofessionals were not looking to switch jobs in 2018 (What will improve, 2018). As hackers continue changing their approaches, healthcare cybersecurity teams continue to be trained and certified in the latest techniques. The most common types of attacks are described in the next section.

Common Types of Cyberattacks

In this section, the most common types of cyberattacks are listed providing a high-level description of what is involved with each type of attack. A basic understanding of these types of attacks is required by cybersecurity leadership to prioritize and focus resources to defend against the highest cost attacks.

- *Cross-Site Scripting*. Software is written by the attacker and included in a Web application where it is executed on different machines. The code steals user IDs and passwords, changes information in documents, and makes unauthorized transfers of money (Niakanlahiji & Jafarian, 2019).
- *Denial of Service (DoS)*. In this type of attack, the hacker makes systems unavailable by sending many requests to get the system backlogged, resulting in slow response or no response (Birkinshaw et al., 2019).
- *Malware*. This is short for *malicious software*, which is software written for malicious purposes. Common types of malware include Trojan viruses, ransomware viruses, and spyware (Vaduva et al., 2019).
- *Man-in-the-Middle (MITM)*. Communication between two computers is intercepted and the attacker can control the communication by reading, changing, or replacing data and will leave no trace (Mallik et al., 2019).
- *Phishing*. This type of attack is typically conducted via email and is the initial step of a larger attack. A fake email is sent out to get the reader to click on a

link to download malware or to harvest credentials. These emails appear to be from legitimate organizations and include a link to a Website that requests information be updated or validated on legitimate-looking Websites. After clicking the link, the unsuspecting user enters their username and password and, potentially, additional information such as address, phone, social security number, and credit card information (Vincent, 2019).

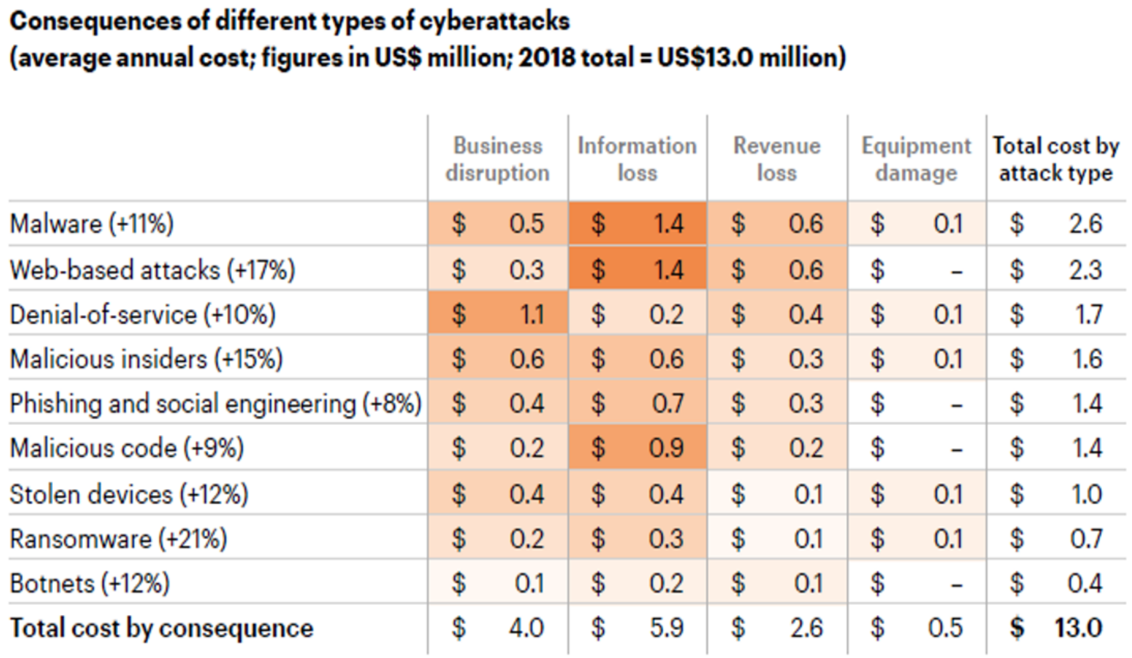
- *Ransomware.* This form of malicious software is used by cybercriminals to lock up a computer and keep it under their control until the user pays for its release. Money is extorted from unsuspecting users by encrypting files, threatening to delete files, denying access to applications, or entrapping them with illegal pornographic material. The user is instructed to submit some form of untraceable payment such as bitcoin; however, payment does not always guarantee the criminals will release the lock (Greene, 2020).
- *Ransomware as a Service (RaaS)*. A new form of ransomware attack where cyberattacks can initiate attacks without technical experience. A portion of the ransom collected by the cyberattacker is sent to the RaaS services provider (Connolly & Wall, 2019).
- *SQL Injection*. This type of application attack is where the hacker gains access to databases by adding a malicious query to a legitimate query at the browser layer, resulting in data being returned that is different than the original query (Volkova et al., 2019).

With these various types of cyberattacks, the cybercriminal is most often seeking financial gain, a dramatic shift from earlier motives of showing off their skills and abilities (Azab & Khasawneh, 2020). Using proactive preventative measures to keep the cybercriminals out of the systems is much less costly than the reactive responses of a security breach where data is compromised (Kamiya et al., 2019).

The costs of a breach can be difficult to quantify, but in the literature, there is general agreement on the types of losses. Figure 3 shows the average annual costs of cyberattacks in the United States for 2018, and the $13 million total cost is split by the type of attack. This is useful information for CISOs when determining where to focus cybersecurity resources and enables them to prioritize resources to the type of attacks with the highest cost. The darker colors indicate higher costs; Malware and Web-based attacks are the highest cost in terms of types of attacks, followed by denial-of-service, and then malicious code. Mitigation strategies focused on reducing these attacks would be the most cost-effective approach if cost is an important factor.

Figure 3

Heat Map Showing Costs by Types of Attacks



Consequences of different types of cyberattacks
(average annual cost; figures in US$ million; 2018 total = US$13.0 million)

	Business disruption	Information loss	Revenue loss	Equipment damage	**Total cost by attack type**
Malware (+11%)	$ 0.5	$ 1.4	$ 0.6	$ 0.1	$ 2.6
Web-based attacks (+17%)	$ 0.3	$ 1.4	$ 0.6	$ –	$ 2.3
Denial-of-service (+10%)	$ 1.1	$ 0.2	$ 0.4	$ 0.1	$ 1.7
Malicious insiders (+15%)	$ 0.6	$ 0.6	$ 0.3	$ 0.1	$ 1.6
Phishing and social engineering (+8%)	$ 0.4	$ 0.7	$ 0.3	$ –	$ 1.4
Malicious code (+9%)	$ 0.2	$ 0.9	$ 0.2	$ –	$ 1.4
Stolen devices (+12%)	$ 0.4	$ 0.4	$ 0.1	$ 0.1	$ 1.0
Ransomware (+21%)	$ 0.2	$ 0.3	$ 0.1	$ 0.1	$ 0.7
Botnets (+12%)	$ 0.1	$ 0.2	$ 0.1	$ –	$ 0.4
Total cost by consequence	$ 4.0	$ 5.9	$ 2.6	$ 0.5	**$ 13.0**

Note. From “The Cost of Cybercrime,” 2019, Ponemon Institute, p. 20. (https://accntu.re/2HbVmgn)

What Are the Types of Costs Involved If Breached?

Across various industries, quantification of the cost of a breach has historically been estimated per record breached. If there was a breach of one million records, it would be much more costly than a breach of 10 records; the bigger the breach, the bigger the cost (Ponemon Institute, 2018). This cost varies according to industry with healthcare being the highest of all industries.

The 2018 estimate for a healthcare data breach is $408 for each medical record compromised and it has been the highest for the past 8 years. The average for all industries is $148 per record (Ponemon Institute, 2018). The estimated per-record costs are shown by industry in Figure 4. The data showing in red is the average over the previous 4 years and the data in blue is for 2017. Figure 5 shows the data for 2018. The healthcare cost per record in 2017 was $380 and in 2018 was $408. These costs are expected to continue to increase.

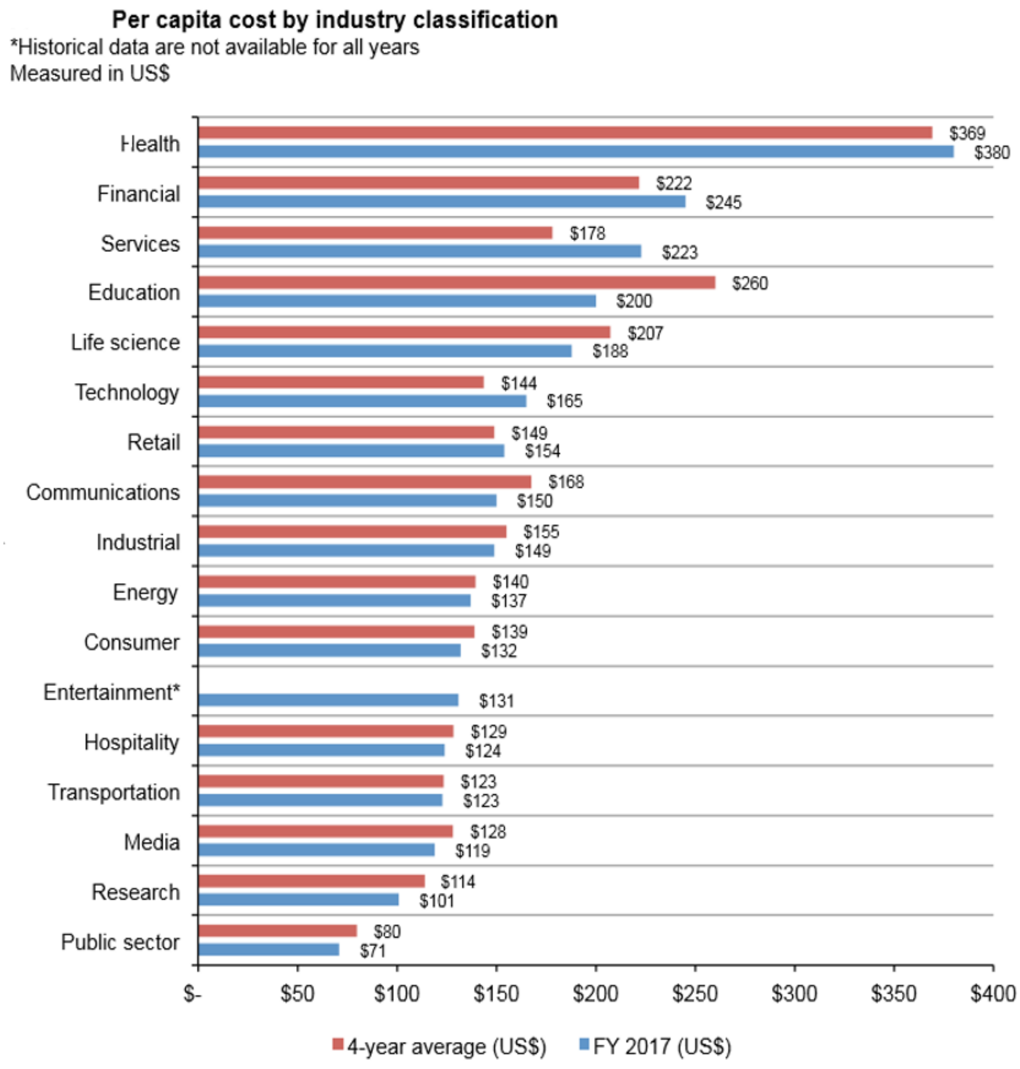
In the report by Ponemon Institute (2018), the numbers were calculated using direct and indirect expenses, and they attempted to maintain consistency across the years. According to the 2018 report,

> Direct expenses include engaging forensic experts, outsourcing hotline support, and providing free credit monitoring subscriptions and discounts for future products and services. Indirect costs include in-house investigations and communication, as well as the extrapolated value of customer loss resulting from turnover or diminished customer acquisition rates. For purposes of consistency with prior years, we use the same currency translation method rather than adjust accounting costs. (p. 8)

And, more recently “For the tenth year in a row, healthcare continued to incur the highest average breach costs at $7.13 million—a 10.5% increase over the 2019 study” (Ponemon Institute, 2020, p. 12).

Figure 4

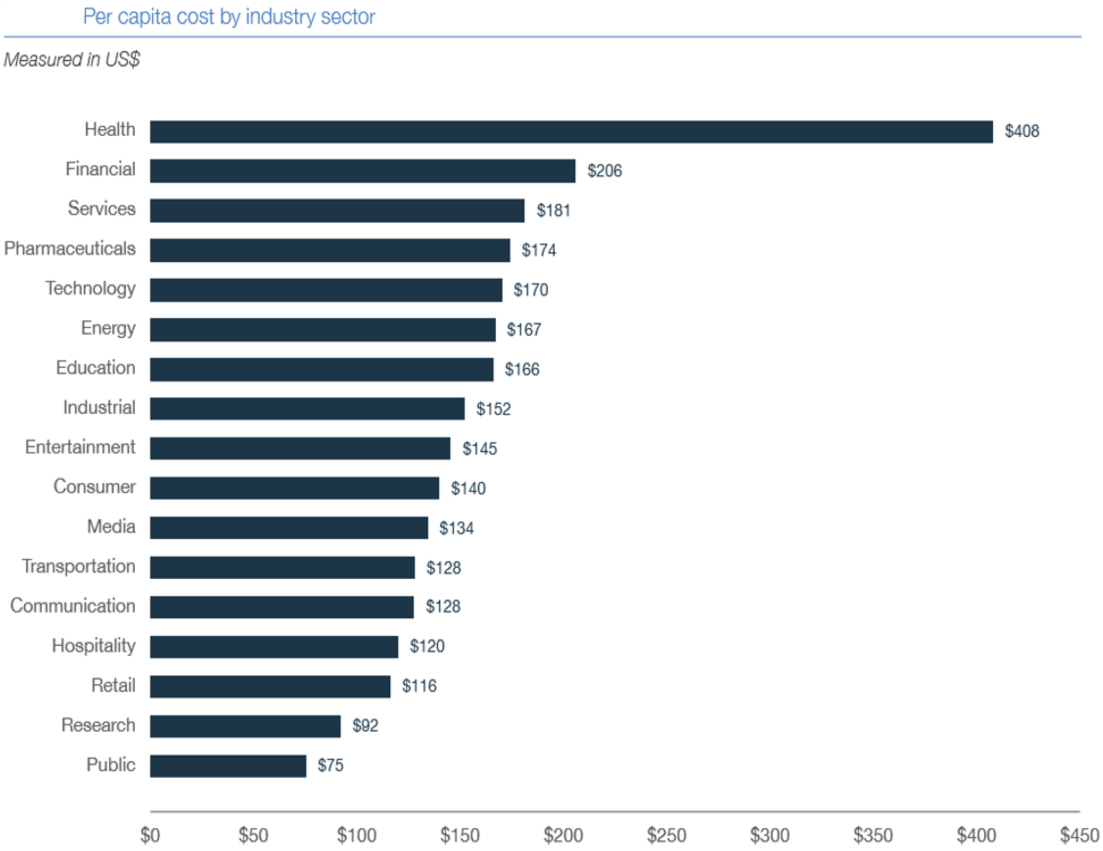
Cost of a Data Breach Per Record by Industry – 2017



Note. From “2017 Cost of Data Breach Study: Global Overview,” 2017, Ponemon Institute, p. 12. (https://www.ibm.com/downloads/cas/ZYKLN2E3)

Figure 5

Cost of a Data Breach Per Record by Industry – 2018



Note. From "2018 Cost of Data Breach Study: Global Overview," 2018, Ponemon Institute, p. 18. (https://www.ibm.com/downloads/cas/861MNWN2)

Calculating the cost of a breach is difficult due to the subjective nature of items (e.g., reputational loss and loss of business). Several authors agreed on the types of costs involved in a breach (see Table 1), with multiple columns of authors indicating many of the same costs.

Table 1

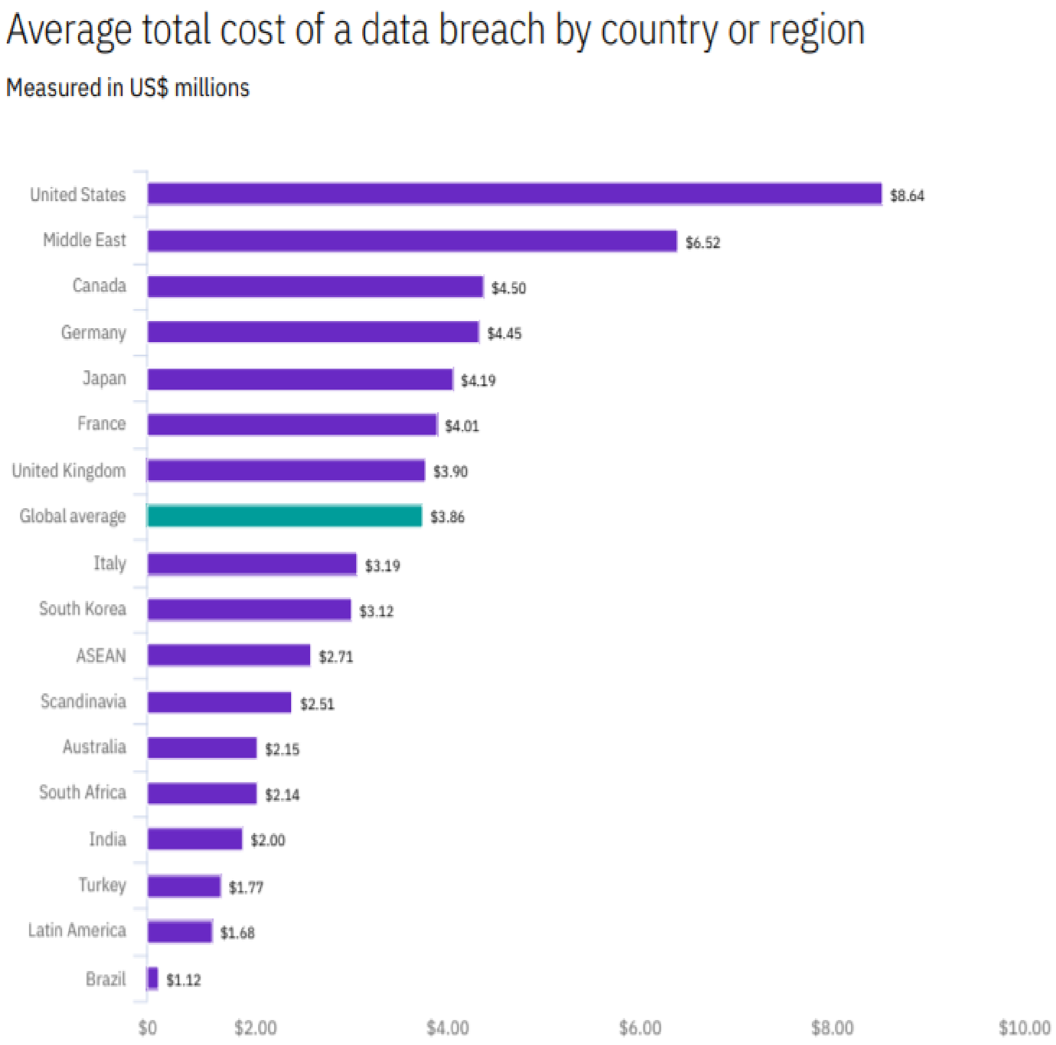
Types of Costs Involved in a Breach Per References in Column Heading

Types of Costs Involved in a Breach	Meisner (2018)	Anderson (2018)	Sivagnanam (2018)	Jalali and Kaiser (2018)	Ponemon (2017, 2018, 2019)
Detection and Escalation, Forensic Investigation	X	X			X
Post-Breach Notification to Victims	X				X
Post-Breach Credit Protection for Breach Victims, Identity Protection Services	X	X	X		X
Attorney Fees/Litigation, Class Action Lawsuit	X		X	X	X
Regulatory Compliance Fines, State, or Federal Penalties	X	X	X	X	X
Cybersecurity Improvements, Remediation	X	X	X		X
Loss of Reputation, Damage to Brand, Loss of Consumer Confidence	X	X	X	X	X
Cyber Insurance			X		X
Business Disruption					X
Information Loss					X
Revenue Loss					X
Equipment Damage					X

The most recent report data from Ponemon Institute (2020) shows that the cost of U.S. data breaches is almost double of other countries (see Figure 6). The assumption is that because we rely on technology much more than other countries, we have much more data stored, and therefore are targeted more frequently, resulting in more attacks.

Figure 6

Average Total Cost of a Breach by Country or Region



Note. From "Cost of Data Breach Report 2020" 2020, Ponemon Institute, p. 5.

(https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/pdf)

Frameworks and Methodologies—HIPAA, NIST, PCI DSS, and SOX

There are various regulations, frameworks, and methodologies that have been developed to help organizations design and implement controls to protect against cyberthreats. Many variations of these standards have been developed; however, rarely do the compliance standards completely safeguard the data from hackers. These standards are discussed in detail in the next section. Table 2 indicates the types of data to be protected for each framework. Organizations select the most applicable framework for the type of data they are protecting. Many times, the selection may include many frameworks to protect different business areas (i.e., credit card processing applications will need to adhere to the PCI DSS requirements, financial data of publicly traded companies must comply with SOX, and healthcare data must follow HIPAA security rule regulations to be compliant). Trying to ensure compliance with all areas is a difficult task. Table 2 summarizes a few of the regulations and frameworks used in healthcare and other environments; it is not all encompassing, but provides a sample of commonly used standards. The following sections provide additional details for these six standards.

Table 2

Sample of Commonly Used Standards

Regulation or framework	Year	Industry	Applicability/Jurisdiction
GDPR	2018	Medical	European Union Law
HIPAA	1996	Medical	Federal Law
ISO 27001	1995	Various	International Standard (not law)
NIST 800-53	2005	Federal Information Systems	Recommended Risk Management Framework (not law)
PCI DSS	2004	Credit Card	International Standard (not law)
SOX	2002	Financial	Federal Law—Publicly Traded Companies

HIPAA

The need to protect healthcare data to ensure security and privacy has expanded along with the EHR implementations, the growth of massive databases, medical devices, and interconnectivity (Jalali & Kaiser, 2018). HIPAA requires specific privacy and security controls to be in place for ePHI to help mitigate the risk of breaches. The controls apply to systems that process, store, or transmit ePHI, and are assessed at the various layers of the technology environments (e.g., application, database, host, network, etc.). The HIPAA security rule requires that an enterprise-wide risk analysis be conducted, starting with an inventory of all assets. The threats and vulnerabilities documented in the risk analysis are risk ranked and then fed into the enterprise-wide risk management plan.

HIPAA regulations state that ePHI includes any of 18 distinct demographics that can be used to identify a patient, and include name; address (including subdivisions smaller than state such as street address, city, county, or zip code); any dates (except years) that are directly related to an individual, including birthdate, date of admission or discharge, date of death, or the exact age of individuals older than 89; telephone number; fax number; email address; social security number; medical record number; health plan beneficiary number; account number; certificate/license number; vehicle identifiers; serial numbers or license plate numbers; device identifiers or serial numbers; Web URLs; IP address; biometric identifiers such as fingerprints or voice prints; full-face photos; and any other unique identifying numbers, characteristics, or codes.

Additionally, HIPAA sets standards for the storage and transmission of ePHI. Media used to store data includes personal computers with internal hard drives used at work, home, or while traveling; external portable hard drives; magnetic tape; removable storage devices, including USB drives, CDs, DVDs, and SD cards; and Smartphones and PDAs. Means of transmitting data via Wi-Fi, Ethernet, modem, DSL, or cable network connections includes email and file transfers.

Many organizations select a framework to meet the legal requirements and implement controls that include areas such as identity and access management, audit logging and monitoring, continuity planning, and configuration management. HIPAA requirements are high level and not as prescriptive as some frameworks. This is advantageous to healthcare companies as being compliant with the regulation is much easier than other frameworks.

NIST 800-53

According to Tariq et al. (2018), NIST Special Publication (SP) 800-53 is a control directory organized within control families to be applied in a federal information system. The initial release was published in 2005; there have been five revisions published since then with the most recent released in 2017. It should be noted that NIST 800-53 is not a federal regulation, but rather a risk management framework that can be implemented in a customizable fashion for various industries to protect IT systems. It is much more prescriptive than the HIPAA security rule, and the organizations that appropriately implement NIST 800-53 are usually considered as compliant with the HIPAA security rule provisions.

The 17 control families in NIST 800-53 include the following, which can apply at various layers (e.g., network, server, application, etc.) in an environment:

- AC: Access Control
- AT: Awareness and Training
- AU: Audit and Accountability
- CA: Security Assessment and Authorization
- CM: Configuration Management
- CP: Contingency Planning
- IA: Identification and Authentication
- IR: Incident Response
- MA: Maintenance
- MP: Media Protection

- PE: Physical and Environmental Protection
- PL: Planning
- PS: Personnel Security
- RA: Risk Assessment
- SA: System and Services Acquisition
- SC: System and Communications Protection
- SI: System and Information Integrity

The foregoing control families have detailed requirements that must be met, or rationale must be provided as to why it is not met. A compensating control can be indicated that shows how the organization has other related controls in place that sufficiently address that specific risk. The NIST 800-53 standard is used in many large companies that rely on IT and need to protect their systems from attack. Per Roy (2020), "It is voluntary and hence can be suitably used by any organization that looks to deal with cyber threats and information breaches, especially in a technology-heavy environment" (p. 1).

PCI DSS

This security standard applies to all entities that store, process, and transmit credit card information and covers technical and operational system components that are included in or connected to cardholder data (Larson et al., 2019). It should be noted that meeting the credit card standard is not required by federal law. The standard requires an annual report on compliance where an in-depth analysis is performed by a certified QSA (Liu et al., 2010). Each of the detailed requirements is assessed to determine if the requirement is adequately met. The 12 high-level requirements are listed below. CISOs utilized the assessment information to determine which areas to focus resources on.

1. Build and Maintain a Secure Network

   Requirement 1: Install and maintain a firewall configuration to protect data.

   Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters.

2. Protect Cardholder Data

   Requirement 3: Protect stored data.

   Requirement 4: Encrypt transmission of cardholder data and sensitive information across public networks.

3. Maintain a Vulnerability Management Program

   Requirement 5: Use and regularly update anti-virus software.

   Requirement 6: Develop and maintain secure systems and applications.

4. Implement Strong Access Control Measures

   Requirement 7: Restrict access to data by business need-to-know.

   Requirement 8: Assign a unique ID to each person with computer access.

   Requirement 9: Restrict physical access to cardholder data.

5. Regularly Monitor and Test Networks

   Requirement 10: Track and monitor all access to network resources and cardholder data.

   Requirement 11: Regularly test security systems and processes.

6. Maintain an Information Security Policy

Requirement 12: Maintain a policy that addresses information security.

SOX

The focus of Section 404 of SOX is on financial data traceability and requires publicly traded companies to provide evidence of audit trails back to the IT systems, software, processes, and sources of transactions that make up the company’s financials (Selig, 2018). When the illegal and fraudulent accounting practices of major corporations such as Enron and WorldCom were uncovered, the federal government enacted SOX, which made top executives criminally liable for inaccurate financial reporting. This law was very controversial and highly debated as many felt the cost to comply was not worth the benefits gained, although there have been some positive effects (e.g., increased earnings and improved internal control systems) (Fischer et al., 2020). The primary focus of SOX is on access controls and software change management in relation to financial systems. It should be noted that the intent was not to stop hackers, but rather to stop insider fraudulent activities. According to Fischer et al. (2020), “SOX greatly contributed to the improvement of quality of financial reporting and of corporate governance as a whole” (p. 108).

GDPR

GDPR is the most recently added law enacted in the European Union, which sets clear principles that apply to all medical data and all healthcare organizations (Mustafa et al., 2019). The GDPR was finalized in May 2016 and became enforceable on May 25, 2018 (van Veen, 2018). The terms *data processors* and *data controllers,* and the roles they play, must be understood to make sense of the 99 articles of the regulation.

According to Hintze (2018), it is important to understand these two terms and the required obligations. The data processors are normally the third-party providers who process the data, and the data collectors are normally the enterprise that collects the data; however, these relationships must be understood for each situation as they can vary (Hintze).

These newly added requirements build on principles, concepts, and themes already in place. The regulation provides the data subject more control over their data. The following are a few important requirements:

- Provides individuals the ability to control their personal data.
- Customizable consent for the individuals.
- Breaches must be reported within 72 hours.
- Information to show compliance with the regulation must be made available (Mustafa et al., 2019. p. 2).

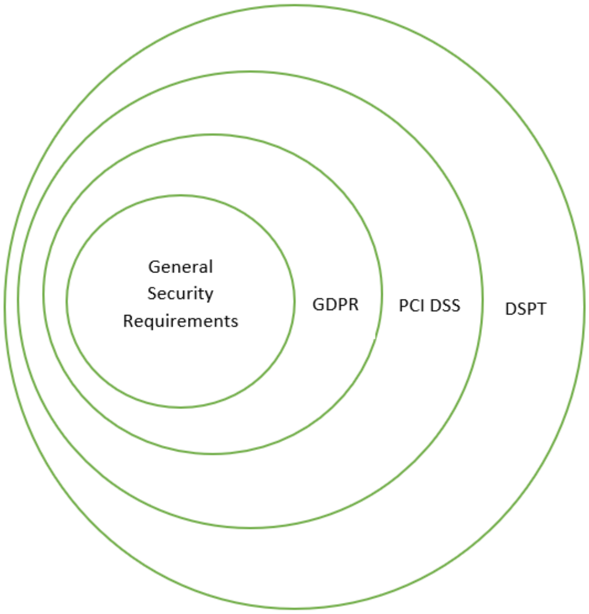
To summarize this section, there are a variety of frameworks and standards to select from when looking to implement IT security controls. There are some overlapping areas in the various frameworks and standards that relay the importance of getting those areas right. The common theme is that they all lack clarity and specificity, making it difficult for organizations to interpret and implement successfully.

What Are the Best Mitigation Strategies?

There is no agreement on strategies that healthcare companies consider desirable, feasible, and important to have in place to mitigate the risk of cyberattacks. It is also not possible to completely remove all cyber risk from an environment. According to Kamiya et al. (2019), “It is effectively impossible to fully eliminate the risk of being hacked” (p. 5). There are recent attempts to create frameworks that encompass various requirements such as Aliyu et al. (2020), who proposed a cybersecurity maturity assessment framework for higher education (see Figure 7). Aliyu et al. included a mapping from each framework for ensuring all requirements are included. This is an approach that will vary according to the industry; however, it is one method to simplify mitigation of risks and meet all requirements and regulations.

Figure 7

Cybersecurity Maturity Assessment Framework



Note. Adapted from “A Holistic Cybersecurity Maturity Assessment Framework for Higher Education Institutions in the United Kingdom,” by A. Aliyu, L. Maglaras, Y. He, I. Yevseyeva, E. Boiten, A. Cook, & H. Janicke, 2020, *Applied Sciences*, *10*(3660), p.10. (https://doi.org/10.3390/app10103660)

Many industries are facing the dilemma of not knowing how to move forward to best protect data, especially when there are complex regulations that apply. Gibson (2020) provided the results of his study and indicated there is no comprehensive strategy to implement cybersecurity for the U.S. Department of Defense (DoD). A Delphi methodology was used to gain consensus from 20 of the DoD cybersecurity experts on the important strategies needed for the next 10 years. Gibson’s study is similar to what this researcher is attempting with this qualitative classical Delphi study; however, the focus of this study is on the healthcare industry.

Table 3 lists the strategies in the first column, and each author that mentions the strategy as important is indicated with an *X* for that row under the author’s name. There are not many overlapping strategies that expose the lack of agreement on strategies in the literature. This list of strategies will provide a starting point for the initial survey questions to have the participants indicate which of these, in their view, are most desirable, feasible, and important.

Table 3

Strategies to Reduce Risk

Strategies	Anderson (2018)	Coventry & Branley (2018)	Atluri (2018)	Happa et al., (2019)	Jalali & Kaiser (2018)	Gibson (2020)
Provide employee education and training	X			X		X
Monitor social media	X					
Strong passwords/multi-factor authentication	X			X		
Establish cybersecurity policy/program	X					X
Conduct risk assessments	X					
Practice good cyber-hygiene (backups, patches, de-identify, encryption)		X				
Design built-in security from the start		X				
Culture of security in patient care, a risk aware culture		X	X			
Cyber insurance		X				
Develop a 3–5-year strategy			X			
Identify and classify all assets			X			
Monitor risk continuously			X			
Build a robust incident response program			X			
Implement encryption				X		
Implement intrusion detection systems (IDS)				X		
Assess and measure harm				X		
Resource availability					X	
External pressure					X	
End point complexity					X	
Internal stakeholder alignment					X	
Cybercriminal activity					X	
Understanding threat landscape						X
Cybersecurity personnel – recruiting, retention, and training						X

It was my hope that this study would begin to fill the gap in the literature and provide an agreed-upon strategy for implementing cybersecurity controls in large U.S.-based healthcare organizations. According to Jalali et al. (2019), another area where the literature is lacking is with physical security (e.g., data center physical controls such as locked doors, security cameras, badges, visitor logs, etc.). Even with increases in cybersecurity spending, there has not been proportional growth in the literature (Jalali et al.). There is one area that was well covered in the literature that includes the articles dealing with the regulations and frameworks. There are solid arguments that indicate compliancy does not always mean systems are secure. Identification of desirable, feasible, and important mitigation strategies will help organizations move in the right direction when implementing cybersecurity controls to protect their data.

Summary and Conclusions

In this literature review, the following questions were answered and various thoughts in the literature provided insight and interesting perspectives on these topics.

- How has technology grown and what impact has it had in healthcare?
- Why is protected health information targeted by hackers?
- What are the most common types of attacks?
- What are the costs involved if breached?
- What are common regulations and frameworks?
- What are the best mitigation strategies?

It is well understood that healthcare technology has grown tremendously over the past 50 years. This growth has had positive effects on healthcare; however, it has spurred an increase in cyberattacks. It is also known that healthcare systems are not well protected and are considered lucrative by hackers. The types of attacks against healthcare companies are well known and continue to change as the tactics used by the hackers change. Costs involved in breaches are high and continue to increase. Regulations and frameworks for compliance have not been able to slow the attacks. The major gap in the literature was that there is no agreement by healthcare IT experts on the best cybersecurity mitigation techniques that are the most desirable, feasible, and important. The next chapter will cover the research method used during the study and details of the study will be described in great length.

Chapter 3: Research Method

The purpose of this qualitative classical Delphi study was to determine how a panel of 25 CISO cybersecurity experts working in U.S.-based healthcare organizations viewed the desirability, feasibility, and importance of IT cybersecurity risk mitigation techniques. This chapter includes details about the research design and the rationale of why this design was selected, the role of the researcher, the methodology to include logic for participant selection, instrumentation, recruitment, data collection procedures, and the data analysis plan. Also included are strategies for ensuring trustworthiness of the study through credibility, transferability, dependability, confirmability, and ethical procedures. The chapter ends with a summary and a preview of Chapter 4.

Research Design and Rationale

The following research question guided this qualitative classical Delphi study: What are the U.S. IT healthcare cybersecurity experts' views on the desirability, feasibility, and importance of effective cybersecurity risk mitigation techniques? The central concept of this qualitative classical Delphi study was to learn from the experts in healthcare cybersecurity what mitigation techniques have worked in their organizations to protect patient data and prevent attacks. The information gathered can then be shared and used across various IT-related industries.

The qualitative classical Delphi design I used in this study was a good fit since iterative surveys gather data about the experiences of others (Brady, 2016). "The purpose of qualitative research is to deepen one's understanding of specific perspectives, observations, experiences, or events evidenced through the behaviors or products of individuals and groups as they are situated in specific contexts or circumstances" (Johnson et al., 2020, p. 143). I attempted to understand the perspectives and experiences of CISO cybersecurity experts working in U.S.-based healthcare organizations.

Mitigation of cybersecurity risk is a complex issue with varying opinions on the most desirable, feasible, and important ways to address these risks. The Delphi design allowed me to bring opposing views together and is especially useful for addressing complex issues (Rayens & Hahn, 2000). This design also allowed for deeper understanding using iterative surveys that were refined for each iteration.

Quantitative and mixed-methods designs were reviewed and considered, but I did not select either one as they are not a good fit for this type of study where the goal is to understand experiences and perspectives of others. Researchers conduct quantitative studies to identify trends or define causal relationships between variables (Lo et al., 2020). There were no trends or variable relationships involved in this study's purpose. Mixed methods studies combine qualitative and quantitative approaches (Lo et al., 2020) and, as such, it is especially complex for first-time researchers to successfully navigate two methods for their first study. This study was best fitted to a qualitative research approach as we have built consensus with the experts' experiences in mind.

Role of the Researcher

The role of the researcher for this qualitative classical Delphi study included planning the study, recruitment and selection of participants, drafting survey questions, creating the SurveyMonkey questionnaires, and sending the survey to the participants. I collected the data and completed the analysis, identified themes, and drafted the second round of survey questions. This process was repeated until data saturation occurred, which was after the completion of the third round of surveys. Ensuring that research question, data, and analysis were consistent and aligned with the original purpose and problem statement was important to remember throughout the study (Bansal et al., 2018).

There were no personal or professional relationships with the recruits as they were contacted from LinkedIn groups focused on CISO cybersecurity experts working in U.S.-based healthcare organizations. Researcher bias had to be managed because my experiences and background could have potentially influenced the way the questions were asked and the way answers were interpreted. Making sure the questions were written clearly and appropriately helped reduce bias (Johnson et al., 2020). Letting the experts provide their perspectives without judgement as to correctness was carefully considered throughout the three rounds of the study.

To avoid conflict of interest and ethical issues, I did not reveal my place of employment to other participants as it could have changed the answers to what they think the federal government was looking for. The participants also may have felt it could be used against their organization during legal investigations. I am a federal contractor for the HHS Office of Civil Rights; I review submitted documentation from breached healthcare organizations to determine adequacy of compliance with HIPAA security rule provisions. I have removed the name of my workplace from all social media accounts, to help keep this information from leaking to the participants. I did not use any information gathered from the study in their workplace, and the participants were not identified by name or by organization in the results of the study. This ensured better answers and a more relaxed environment for the study, enabling truthful answers.

Methodology

Participant Selection Logic

As described in Chapter 1, the study population included CISO cybersecurity experts in large U.S.-based healthcare organizations who had a minimum of 10 years of experience. Initially, 25 subjects were selected using purposeful sampling. It was expected that some participants would not complete the entire qualitative classical Delphi study, and the target was to have 20 participants finish all rounds of the electronic survey questions. During the recruiting phase, the subjects were informed of the time expectation, not to exceed a total of 1 hour for all three rounds of surveys. An incentive was provided for those who finished the three rounds of the study—a free copy of the results of the research.

The sample size of 25 is average for qualitative research using the Delphi method. There are no hard and fast rules to the required number, but a range from three to 45 is indicated as sufficient. One criticism of qualitative research is the small sample sizes; however, Tutelman and Webster (2020) indicated that the small size is a core characteristic since the data are intended to provide rich and deep exploration rather than the broader quantitative studies. Finding 25 qualified subjects did cause minor issues, but there were several ways used to gain interest in participating in the study.

The potential subjects were sent a message via the LinkedIn groups centered on cybersecurity and healthcare. Permission from the group owners was requested and the initial request letter was posted by the group owner to all group members. One additional method not used to identify potential participants was through the SurveyMonkey option to recruit participants; that method would have incurred a large cost but could have saved time in this process. By conducting a search on Google for CISO cybersecurity experts working in large U.S.-based healthcare organizations, I gained access to contact information such as email addresses through LinkedIn. These email addresses were also used to search for additional CISOs using a snowball technique since the LinkedIn group did not provide at least 25 participants.

The traditional snowball sampling technique was used to identify additional subjects as it has proven to be an effective and no-cost method (Chambers et al., 2020). The participants were queried to see if they had additional names and email addresses of other healthcare CISOs who might be interested in taking part in the study. The participants forwarded the email request to other CISOs. Getting emails from people you know is much more effective than getting emails from unknown doctoral students.

The confirmation to ensure selected participants met all criteria was included in the first part of the survey questions for Round 1. In addition, the informed consent information was provided in the first survey. The participant was required to indicate that they understood the information provided and were willing to proceed with the study.

Instrumentation

The data collection instrument for the three rounds of surveys was an electronic survey that I created using SurveyMonkey. The specific link was emailed to each participant for each round, and I used a spreadsheet to track dates the survey was sent and the dates responses were received. These researcher-developed surveys were based on the information in the Chapter 2 literature review and directly reflected the research question. The desirability, feasibility, and importance of cybersecurity mitigation techniques were the central focus of the first survey. A high-level, generalized list of mitigation strategies (as shown in Table 3) was provided in the form of questions, and the participants used multiple choice answers to indicate the level of desirability, feasibility, and importance along with choices of *None of the Above* and *All of the Above*. In addition, the Round 1 survey included a final open-ended question where the participants were able to add free text comments about any missing strategies they felt were desirable, feasible, and important.

These mitigation strategies I selected from the literature for the first-round survey included the following: employee education and training; strong passwords and multi-factor authentication; monitoring mobile devices and social media; establishing a cybersecurity program; and performing regular risk assessments (Anderson, 2018). The strategies indicated by Coventry and Branley (2018) included good cyberhygiene, built-in security from the start, culture of security, and cyberinsurance. Atluri (2018) believed having a 3- to 5-year cybersecurity plan, asset management programs, continuous monitoring, and incident response programs were important strategies. Education, encryption, intrusion prevention and detection, and assessments of harm were the main recommendations from Happa et al. (2019). Ensuring cyber resource availability via recruiting, retention, and training was important for Jalali and Kaiser (2018) and Gibson (2020).

Procedures for Recruitment, Participation, and Data Collection

This section includes the plans of how subjects were requested to join the study, the level of their participation and data collection mechanisms. For this Delphi design study, only the initial survey questions were created prior to the qualitative classical Delphi study. The results from the Round 1 survey were used to create the Round 2 survey questions and, likewise, the Round 3 survey questions were created based on the results of Round 2 questions. This allowed the results of each round to drive the direction of the study.

- From where was data collected?
    - Participants completed electronic surveys. They were recruited via LinkedIn social media groups, Google searches for contacts, and additional participants were requested using the snowball technique.
    - Qualification criteria were confirmed during the informed consent process.
    - Links to each round of the three electronic surveys were emailed individually to each of the qualified participants who provided informed consent by completion of the survey.
    - It should be noted, keeping in mind the safety of the participants, that this method reduced COVID-19 risk as there was no face-to-face contact made for data collection.
- Who collected the data?
    - I used a software tool, Survey Monkey, as the collection mechanism.

  - Survey Monkey allowed a free version for up to 10 questions and 40 participants, and an unlimited version for a low monthly fee.
  - I simulated a survey to become acquainted with Survey Monkey capabilities and format for results with the free version as preparation. For the study surveys, the paid subscription was required as there were more than 10 questions.
- Frequency of data collection events.
  - Every 2 weeks, a round of the surveys was planned to be sent, expecting a month and a half in total for the three rounds. It took longer than expected to get 25 participants, so this was slightly delayed,
  - An Excel spreadsheet was used to track communication with the participants (i.e., date survey sent, email address sent to, date response received, etc.).
  - The participants were asked to provide responses within 48 hours of the surveys being sent to help expedite the study process. Not all participants were able to complete the surveys within the requested timeframe.
  - Nonresponses were followed up with an additional reminder email after 48 hours, including the link for unanswered surveys.
  - The delay in the turnaround time did not allow much time for me to review and analyze the data to prepare the next round of survey questions.
- Duration of data collection events.

  - Each survey was designed with 20 questions or less, to be answered within 10 to 15 minutes each.
  - The expectation of a time commitment for each participant was that a maximum total of 45 minutes was needed for the three surveys. This was explained to potential participants to help reduce attrition later (Avella, 2016).
  - The expectation was originally that there would be 2 weeks between each survey, which was one and half months of collection activity. This was delayed, with the duration taking over 2 months for completion.
  - I took time off work during this survey timeframe to focus on the study, analyze the results, and generate the next round of surveys.
  - The intent of the quick turnaround was to help reduce the chances of participants dropping out of the study.
- How were data recorded?
  - Survey Monkey results, including the graphs of the results, were stored in a secure manner on an Excel spreadsheet and other documents as needed.
  - Open-ended questions and answers were collected and consolidated in preparation for analysis where recurring themes were identified.
- Follow-up plan if recruitment results in too few participants.
  - When there were not enough participants, I queried the confirmed participants using the snowball technique to recruit additional members.

  - I searched Google for large health company CISOs for contact information.
  - Since the recruiting numbers were lacking, a request was made to the Institutional Review Board (IRB) that was approved to lower the dollar amount of healthcare companies' annual revenue, which widened the search parameters. The result was that CISOs from a wider group of healthcare companies were considered.
  - A lower number of participants were acceptable; the acceptable range of participants in the Delphi method is from 10 to 100 participants and there is no agreed upon standard (Avella, 2016).
  - In the worst-case scenario, I could have revised the study and reconsidered other methods and designs that would not have required as many participants.
- Explain how participants exit the study (e.g., debriefing procedures).
  - After the third round of survey questions were completed and analyzed, each of the participants received an email indicating the study had been completed and included any needed debriefing instructions at that time.
  - When the results are finalized within the published dissertation, a free copy will be emailed to them as a token of appreciation for participating.
- Describe any follow-up procedures such as requirements to return for follow-up interviews.

- If additional information is required, the additional rounds of surveys could add clarifying questions, or an email could be sent to the entire pool of participants to clarify.

Data Analysis Plan

For the data collected in Round 1, I attempted to determine which mitigation strategies were considered as most desirable, feasible, and important. Some mitigation strategies were considered as all three and others were none of the above. Each question in the survey identified a high-level strategy and the participants answered with one of these five multiple-choice answers: *desirable, feasible, important, all of the above,* or *none of the above*. This made data analysis very straight forward as the strategies with the highest numbers of participants indicating the desirable, feasible, important, or all of the above were included for additional questions in the next survey. There was one open-ended question that allowed participants to add to the list of strategies. This is where coding and categorization of the codes into themes was a logical next step and was documented on a spreadsheet.

The additional rounds of surveys were used to further understand the details of how participants view the mitigation strategies and confirm understanding of the responses. The data for each round drove additional collection for the following survey.

Connection of Data to a Specific Research Question

The data collected was aligned specifically with the research question: What are the IT healthcare cybersecurity experts' views on the desirability, feasibility, and importance of effective cybersecurity risk mitigation techniques? I developed questions to include 18 identified strategies from the literature review, and the participant needed to indicate if each strategy is viewed as *desirable*, *feasible*, *important*, *none of the above*, or *all of the above*.

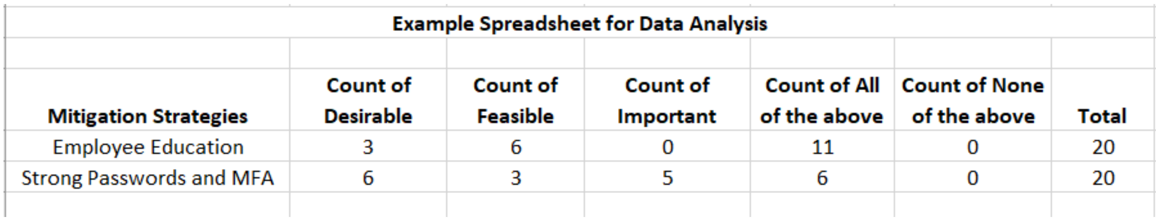
Type of Procedure for Coding

The type of data being collected was multiple-choice answers from the survey questions and one open-ended question. The data was captured in SurveyMonkey, downloaded, and saved into Excel spreadsheets that were used to better understand the data. I am experienced with Excel and very comfortable with conducting analysis using functionalities provided in Excel. A codebook was recorded in Excel indicating the name of the code, the coding cycle, and a clear definition of the code with enough detail included so that others can follow the directions for coding.

The spreadsheet was set up to easily summarize results to enable getting a count of each strategy (e.g., employee education could show that three participants thought it was desirable, six participants thought it was feasible, and the remaining participants thought it was all three: desirable, feasible, and important). This was used to create Excel graphs to easily visualize analysis results for the readers. This graph got visually busy with all 18 strategies and SurveyMonkey already provided a graph of the results for each question.

Figure 8

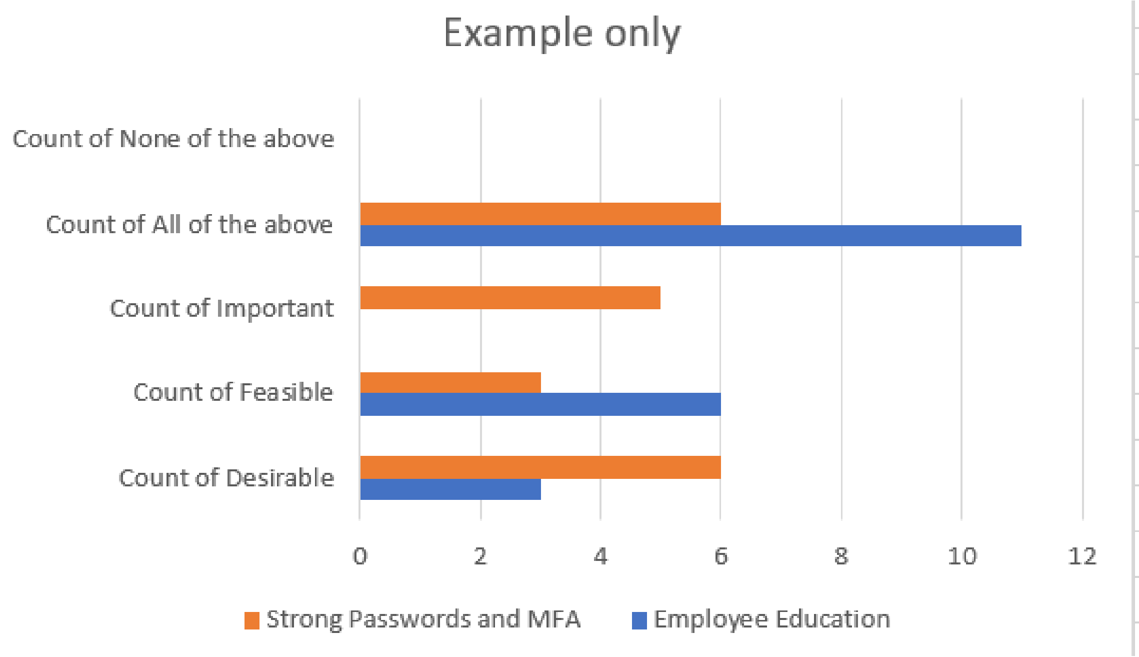
Example Spreadsheet for Results Analysis



Example Spreadsheet for Data Analysis						
Mitigation Strategies	**Count of Desirable**	**Count of Feasible**	**Count of Important**	**Count of All of the above**	**Count of None of the above**	**Total**
Employee Education	3	6	0	11	0	20
Strong Passwords and MFA	6	3	5	6	0	20

Figure 9

Example Graph of Results



Any Software Used for Analysis

NVivo, which provides analysis on word frequencies and key words, was going to be used for analysis of the survey results where open text answers were provided. I determined that the cost of NVivo was too high, and the analysis could be completed in spreadsheets. As the survey data was captured in a text format, there was no need to transcribe from spoken words into written text. Member checking to ensure trustworthiness was conducted by sharing part or all of the previous survey round results with the participants to ensure honest and accurate interpretations. Results were organized within the codebook that was maintained using Excel for each round. To ensure all answers were included, total counts were checked to validate the answers equal the number of the participants.

The open text answers introduced new strategies into the list that were included in the next round of surveys. Coding was conducted based on the survey results, and higher-level themes emerged from the coding activity. Round 2 was used to further confirm the understanding of the results from Round 1 and focused deeper on the themes that were emerging. The point of saturation was not met after the second round, so the third round of surveys was the final list of questions to confirm reliability and trustworthiness of the data collected.

Manner of Treatment of Discrepant Cases

There were no responses that were illogical or inconsistent; therefore, there was no need to retain and note as needing additional information or to add clarifying questions in the subsequent survey rounds.

Issues of Trustworthiness

Credibility

Understanding what makes a study credible and how it leads to trustworthiness helped me to determine which strategies were most appropriate for this qualitative classical Delphi study. Korstjens and Moser (2018) indicated that credibility relates to the truth value and whether the interpretation correctly reflects the participants' views. I identified two ways to improve the credibility of the results including triangulation and member checking. These two internal validity methods are briefly described below, along with a description on how these were applied to this qualitative classical Delphi study.

Triangulation

Lemon and Hayes (2020) defined triangulation as "a qualitative research strategy to test validity through the convergence of information from different sources" (p. 605). In this qualitative classical Delphi study, the different sources were the diverse group of study participants. Three rounds of surveys provided convergence of mitigation strategies that are the most desirable, feasible, and important. This convergence emerged after synthesizing the similarities and differences of how the participants viewed risk mitigation strategies during the analysis phase after the data had been collected. The software tool utilized to assist with this triangulation and convergence of results included an Excel spreadsheet for each round.

Member Checks

To help ensure correct interpretation of data analysis, results were sent back to the participants to have them check for accuracy during subsequent rounds; no discrepancies were identified, and no adjustments were required (DeCino & Waalkes, 2019). The Delphi research design takes results from the first round of the surveys to develop the second round of questions. If the first-round results are misinterpreted, the direction of the study goes off course. It was beneficial to member check each round as the study progressed to ensure correct interpretation of results.

Transferability

The results of the study are transferable to other industries and other physical locations. Transferability in qualitative research suggests that findings from one study can be applied to other settings or groups of people (Daniel, 2019). For this study, the findings are applicable to industries other than healthcare because IT is used in almost all industries, and protection against cyberattacks is generally the same for all organizations. Protecting data from hackers is a topic that is of interest worldwide and results are applicable regardless of physical location.

The content in the surveys and the findings was written at a level so it was understood by not only the participants, but also understood by others who may want to replicate the study in other industries or geographical locations. Methods used to recruit the participants were described in detail to allow for others to easily replicate. The list of desirable, feasible, and important methods to reduce risks applies to a broad audience and is not limited to only U.S.-based healthcare organizations.

Dependability

Audit trails were used to ensure the process of the study was conducted in such a way that the results can be considered dependable. I kept records throughout the study to allow for an independent audit of the study after completion. Amin et al. (2020) provided six categories of information that are useful to conduct an audit: (1) raw data, including recordings, field notes, and other documents; (2) data reduction and analysis products, including summaries; (3) data reconstruction and synthesis product, including themes, results, conclusions, and reports; (4) process notes, including notes related to methods used and trustworthiness; (5) materials addressing intentions and dispositions, including reflexive notes; and (6) instrument development information, including pilot forms and observation charts. These items were documented throughout the three rounds of surveys and were saved into an audit folder for easy retrieval at the time of the audit to prove dependability of the results.

Confirmability

Trustworthiness of study results can be achieved through confirmability. Chung et al. (2020) indicated confirmability is the extent to which the same results can be achieved by others through replication—the level that other studies can confirm the same results. When researchers document clear details about their data analysis procedures (i.e., how data became codes and how codes became themes), the confirmability is verifiable. For this qualitative classical Delphi study, I ensured detailed documentation of the processes for each stage of the study as detailed in the audit trail section. This information could be used by others to replicate the study.

Ethical Procedures

The IRB for organizations has the responsibility to ensure human participants involved in studies are treated ethically. White (2020) pointed out that IRBs have a federally mandated responsibility to review research studies to ensure the intended protocol meets the ethical guidelines before human subjects can be enrolled in the study. Walden’s IRB requires research students to complete the Protecting Human Research Participants training prior to initiating the study. Also, informed consent documentation for each round of the surveys and for all participants was required before involvement in the research.

There are three main components to the informed consent process: information, comprehension, and voluntariness (White, 2020). Participants were provided basic high-level information about the purpose of the study, including any risks. The form was written at the level of a participant’s understanding and ensured there is an understanding that participation in the study is voluntary and included an option to drop out of the study at any time without penalty.

Ethical concerns related to recruiting and data collection were reviewed and approved by the IRB (03-01-22-0125109) prior to initiating the study. In this qualitative classical Delphi study, participant names and organizations were kept confidential. I assigned a unique identifier to each participant and was the only person to know who the participants were. The spreadsheet to map this information was stored encrypted on a flash drive in a safe located in my home.

No participant withdrew from the study; however, if they had, the information provided from that participant would have been deleted, including any survey responses and any other details specific to that participant. This was to ensure that privacy and confidentiality were maintained. Protection of the data after collection included encryption and archival for 5 years to ensure appropriate secure storage of data and study details.

Summary

Chapter 3 included the research design and rationale, the role of the researcher, and the methodology details. In the methodology details section, participant selection logic, instrumentation, procedures for recruitment, participation and data collection and the data analysis plan were explained. The final section of this chapter described issues of trustworthiness, including credibility, transferability, dependability, confirmability, and ethical procedures.

Chapter 4 includes the details of the execution of the study, containing the setting, demographics, data collection, data analysis, evidence of trustworthiness, results, and a summary of the chapter. The data is presented in tables and graphs for all three rounds of the surveys and the survey results were provided as appendices.

Chapter 4: Results

The purpose of this qualitative classical Delphi study was to determine how a panel of U.S.-based healthcare CISO cybersecurity experts viewed the desirability, feasibility, and importance of IT cybersecurity risk mitigation techniques. The following research question guided this qualitative classical Delphi study: What are the U.S. IT healthcare cybersecurity experts' views on the desirability, feasibility, and importance of effective cybersecurity risk mitigation techniques? This chapter includes details for all three rounds of the survey with sections on the pilot study, research setting, demographics, data collection, data analysis, trustworthiness evidence, and the study results.

Pilot Study

This study did not require a pilot study as the instructions and questions for the first round of the surveys were very straightforward. Creswell and Creswell (2018) indicated that pilot testing improves the questions, format, and instructions for the instrument. The participants selected were experienced CISOs and were able to comprehend the straightforward instructions and each of the questions without difficulty. The participants were able to complete the first survey within 5 minutes. In addition, I had used SurveyMonkey in the past and was familiar with the capabilities of the survey tool; therefore, I did not feel the need for a pilot test.

One lesson learned in Round 1 of the surveys was that some questions were possibly better suited to have used the check box format rather than using the multiple-choice format. The participants may have wanted to select a combination of choices, rather than just one choice. As an example, the participants may have wanted to indicate that a strategy could be desirable and feasible, but not necessarily important. A pilot test might have identified this issue and allowed for a change in the question formats. Where applicable, the subsequent rounds of surveys utilized the checkbox format rather than the multiple-choice format.

One change was made during the recruiting phase, which increased the number of potential participants by lowering the annual revenue for the targeted healthcare organizations. However, a pilot study would not have identified this recruiting issue. The change was approved by the Walden IRB and resulted in finding a total of 27 participants to complete the survey for the first round. This was two more than the originally planned number of 25 participants.

Research Setting

During the study, many conditions may have influenced the participants' interpretation and responses. These conditions include the impact of the COVID-19 pandemic, increases in malware attacks utilizing survey links, political divisiveness, and racial tensions. None of these conditions were raised by the participants as affecting their responses. The impact of these conditions on the results appears minimal for this study but is included as an awareness of the conditions at the time.

The COVID-19 pandemic has influenced the healthcare industry in many ways. Healthcare workers have been exposed to unprecedented stress by running over capacity limits, not having personal protective gear, and helplessly experiencing the enormous loss of life (Ripp et al., 2020). Financial losses due to lack of elective surgeries and appointments have been devastating financially to many healthcare organizations. One study indicated a decrease of 50% in clinic volume and a 76% decrease in procedures (Caruso et al., 2021). Strains on healthcare organizations caused by the pandemic were beginning to decrease at the time of the surveys. COVID-19 has also been taken advantage of by hackers to target unsuspecting users.

There have been increases in hacker attacks using surveys that are emailed to trick users into providing personal information to the hackers. This could have negatively influenced the response rate for this study, as participants may have suspected the research surveys to be hacking attempts. On March 31, 2021, the U.S. Department of Justice (2021) sent a warning providing public information about the fake COVID surveys.

Multiple other conditions may have impacted survey results. Civil unrest has escalated across the United States since the death of George Floyd, resulting in racially motivated riots and protests in major cities. Unemployment rates have skyrocketed because of the pandemic. Mental health issues continue to increase and went unaddressed as resources were not available. Shootings have increased. Large numbers of immigrant children are showing up at the U.S. borders and are being mistreated. These items may have indirectly and minimally impacted the thought processes and survey responses from healthcare cybersecurity expert participants.

Demographics

Participants were limited to individuals in the United States who had healthcare CISO (or equivalent) experience. The number of years of experience of 10 years was targeted for the study; however, some of the 10 years may have been in companies that were not related to healthcare. I vetted all recruits initially by reviewing LinkedIn profiles before sending the survey invitation to them. Two areas were reviewed: the individual's career history and the annual revenue of the healthcare organization. An internet search was conducted on financial information for the organization for the individuals who met the experience requirement. Some participants' career histories of the past 10 years were not all specifically in healthcare organizations; however, skills of cybersecurity cross over industries. There was no survey response disregarded based on the response to the first question of the Round 1 survey, the number of years in healthcare CISO positions.

Data Collection

The surveys were created in SurveyMonkey and sent electronically to participants for all three rounds. Table 4 summarizes collection information for each round of surveys. There were 27 participants who responded to Round 1 of the surveys; Round 2 included 20 participants, and Round 3 included 18 participants.

The first round of surveys was sent beginning March 7, 2021, and concluded on April 10, 2021. The second round of surveys was sent beginning April 17, 2021, and ended on May 2, 2021. The third round of surveys was sent beginning May 6, 2021, and ended on June 3, 2021. Data from the surveys were stored in SurveyMonkey, downloaded to a folder on my computer, and backed up with an encrypted thumb drive.

Table 4

Data Collection Summary

Survey round	Responses	Start date	End date	Days
1	27	3/7/2021	4/10/2021	34
2	20	4/17/2021	5/2/2021	15
3	18	5/6/2021	6/3/2021	28

Round 1 Survey Data Collection

For Round 1, the initial recruiting message was sent on March 3, 2021, to two CISO LinkedIn groups, resulting in no responses. As the plan indicated in Chapter 3, Google searches were conducted. The searches identified articles with Healthcare CISO names and their organizations. Search terms included *healthcare CISO, health CISO, med CISO, and clinic CISO*. The CISOs in healthcare organizations with annual revenue of $50 billion or more were identified as potential recruits.

LinkedIn profiles of these vetted recruits were reviewed to ensure they had at least 10 years of CISO experience. If they met the criteria, I made a LinkedIn connection request with a short message. When the LinkedIn connection request was accepted by the individual and they provided their email address, I sent them the survey via email. The consent form was included with each survey and, if they consented, they would continue to fill out the survey. If they did not consent, they exited the survey without completing it. It is not possible to determine how many participants read the consent form and decided not to participate versus the number of individuals who had chosen not to even open the survey. Also, there were a few emails that were not received by the participants and, for those individuals, a link directly to the survey was sent using LinkedIn's private message function.

On March 18, 2021, 11 days later, after only having seven completed surveys, I submitted a Walden IRB change request for the search criteria to be widened to increase the number of eligible participants. I had overestimated the number of healthcare organizations with annual revenues of $50 billion or more, so I requested that the selection criterion for the healthcare organization's annual revenues be changed from $50 billion to $50 million. This change was approved by the Walden IRB on March 19, 2021, and the result was that the pool of recruits was much larger.

Google searches were conducted again, filtering out and eliminating those organizations with under $50 million in annual revenues. Locating contact information for each CISO was also conducted using LinkedIn. For the CISOs in organizations with over $50 million in annual revenue and who had over 10 years of CISO experience, I sent a LinkedIn connection request to 257 individuals inviting them to participate in the study. Of those, 63 (25%) responded positively with LinkedIn connections and 27 of these 63 (43%) completed the Round 1 survey.

The number of participants who completed the first survey was 27 on April 7, 2021, 30 days after the beginning of the Round 1 survey effort. This exceeded the goal to have 25 participants for this first round. On April 10, 2021, the Round 1 survey was closed. The raw data were downloaded from SurveyMonkey and stored in the audit trail folder. Files containing participant names and email addresses were named to indicate that they were unredacted versions. A copy of the folder was made and saved to an encrypted thumb drive.

Round 2 Survey Data Collection

After analysis of Round 1 data, the Round 2 survey questions were formed, drafted, and sent for Walden's IRB review and approval. On April 16, 2021, I received IRB approval for the questions, and on April 17, 2021, I sent the survey using SurveyMonkey to the 27 respondents who had responded in Round 1. The survey progressed and was closed on May 2, 2021, after receipt of 20 responses in 15 days. The raw data from Survey 2 were downloaded from SurveyMonkey and stored in the audit trail folder, again using naming conventions to indicate unredacted information about the participants. This folder was backed up to an encrypted thumb drive.

Round 3 Survey Data Collection

After analysis of Round 2 data, the Round 3 survey questions were formed, drafted, and sent for Walden's IRB review and approval. On May 5, 2021, I received IRB approval for the questions and on May 6, 2021, sent the survey using SurveyMonkey to the 27 participants who responded in Round 1. The survey progressed and was closed on June 3, 2021, after receipt of 18 responses in 28 days. Although the original goal of 20 responses had not been met, multiple reminders about the survey had been sent to the participants and went unanswered. Therefore, I decided to close out the survey. Similar to the first two rounds, the raw data were downloaded, stored, named to indicate unredacted data, and saved to the encrypted thumb drive.

This section described the details for data collection. Each of the three rounds of surveys included similar data collection steps. The data for each round were collected using SurveyMonkey and then analyzed to create the next set of questions for the subsequent surveys. The data analysis is described in detail in the next section.

Data Analysis

In this section, the procedures for analyzing each round of survey data are reviewed in detail. The data analysis utilized the SurveyMonkey formatting of the results and was heavily relied on during the analysis. Graphs to visualize the data were automatically produced by SurveyMonkey and I utilized Microsoft Excel to code, categorize, and determine the final top three strategies.

Each survey round had a goal of reducing the number of strategies (i.e., codes, categories, and themes) for the following round. In the Appendices, the questions and answers are provided in a manner that protects the identity of the participants and their organizations. In addition, the coding activity that led to higher level categories and themes is provided in Appendix H. Discussion of analysis activities are included for each round in the following three sections and are summarized in the final paragraph.

Round 1 Survey Data Analysis

The goal of Round 1 survey data analysis was to reduce the number of the original 18 cybersecurity remediation strategies from the literature review and create the Round 2 survey questions. Initial codes included for the survey questions in Round 1 for Questions 2–19 are the strategies that came from the literature review. In Appendix H, the coding table, the data collected during the survey show the scores calculated from the participant responses. The notes from analysis are also included in the coding table showing strategies to be included in the Round 2 survey questions. The participant responses from the open text question for Round 1 Question 20 are included in Appendix C also.

Graphs of Round 1 responses were automatically provided from SurveyMonkey and are shown for the 20 questions in Appendix C. After reviewing the scores for each strategy, nine of the highest scoring strategies were identified to be carried forward to the next survey. Two similar strategies—backup and recovery strategy, and cyber hygiene strategy—were determined to overlap. The cyber hygiene strategy was broader and included backup and recovery; therefore, these two strategies were merged. There were eight strategies carried forward into Round 2 survey questions. Nine strategies were determined to not be carried forward based on the scores in participants' responses. (See Table 5 for details regarding Round 1.)

The most important factor in the analysis to carry strategies forward was the number of responses that indicated all three of the choices: *desirable*, *feasible*, and *important*. For the responses where 13 or more participants indicated the strategy as *All of the Above*, the strategy then moved into Round 2. If the number of responses was less than 13, the strategies were not moved forward into the next round. One exception was a strategy that was not carried forward, the culture of risk awareness; it had 13 participant responses that indicated an answer of all three. However, the numbers of desirable, feasible, and important responses were much lower than those for other strategies, so it was not carried forward as a strategy for Round 2.

For the open-ended text question in Round 1 (Q20), there were 16 comments from the participants. These were downloaded from SurveyMonkey into a spreadsheet and formatted into columns and rows. A column for grouping similar items and a column for the category was added to assist with analysis. Using an Excel function, a filter was applied to all columns to allow me to focus on one category at a time. One change from the original data analysis plan is that I did not utilize NVivo. NVivo was not required as Excel was sufficient for the analyses, and the cost of the NVivo tool was not justifiable for straightforward analysis.

Details including the questions and the responses of the Round 1 survey are included in Appendix C. Analysis completed for Q20 are also included. The higher-level categories that emerged from Round 1 were included as survey questions in Round 2.

Round 2 Survey Data Analysis

The new categories uncovered in Round 1 were used for questions in Round 2 to get additional insight from the participants. The participants were provided a list of eight strategies (codes) to prioritize for Q1 in Round 2. And Round 2 Q2–Q11 included the newly identified strategies (codes) that the participants provided in the Round 1 Q20 open text responses. For Round 2 Q12, there was one open-text response.

The highest scoring eight strategies from Round 1 were presented to the participants in Q1 of Round 2 as a list. The participants were asked to rank them in order from 1 (highest) to 8 (lowest) based on the desirability, feasibility, and importance. SurveyMonkey provided the data in an easily digestible format (see Appendix E). There was no additional analysis required for the first question.

The remaining 10 questions in Round 2 asked the participants to indicate whether the new strategies were *desirable*, *feasible*, *important*, or *none of the above*. The format of these 10 questions used checkboxes rather than multiple choice, which provided the participants a way to indicate their choices more appropriately. The data were collected and entered in Table 6 in the Round 2 Survey Results section. Those with the lowest scoring numbers are indicated in italicized text and were eliminated from moving forward into Round 3. There were five strategies carried forward that were merged with the eight strategies. The result was a list of thirteen strategies to be included in the survey for Round 3.

Round 3 Survey Data Analysis

The final round of survey questions consisted of Q1 which was a list of 13 strategies to be prioritized by the participants. Appendix G shows the strategy scores in ranking order, highest to lowest. Round 3 Q2 was the final chance for participants to provide feedback or questions, and there were eight responses. I provide comments about each response in Appendix G.

The third round of surveys included two questions. The first question requested the participants to order a list of 13 strategies from 1 (highest) to 13 (lowest) based on the desirability, feasibility, and importance. The SurveyMonkey results of this ranking are shown in the Round 3 Survey Results section. The top three strategies were identified based on the scores shown. The second question was an open text box where participants could provide feedback or ask any questions they might have. There was no need for in-depth analysis or coding for this round, SurveyMonkey provided the results graph and the data (see Appendix G).

To summarize the data analysis of all three rounds, the original list of strategies from the literature review started with eighteen items on the list for Round 1. After analysis of Round 2 data, these eighteen items were reduced to eight strategies. The additional strategies from the 10 questions in Round 2 were merged into the list, and this increased the number of strategies for Round 3 to thirteen. After review of the Round 3 data, participants ranked the strategies, and the top three strategies identified through the survey responses included:

1. Establishing a cybersecurity program;
2. Strong passwords and multifactor authentication; and
3. Cybersecurity hygiene (backups, patching, recovery testing, etc.).

The top three items were the final result of the study. The experts ranked these the highest in terms of desirability, feasibility, and importance after considering multiple strategies in the previous rounds. The trustworthiness of the study results is considered in the next section.

Evidence of Trustworthiness

Credibility

As described in Chapter 3, credibility strategies for this study included triangulation and member checking. Triangulation and convergence of information were attained through three rounds of survey responses. Member checking was utilized as each round of surveys repeated back information from the previous round. As an example of feedback, one comment from a participant indicated the results were not as they had expected: “Surprised data protection, including tested backups isn’t on this list.” However, backups were included on the list in the cybersecurity hygiene category, and the term *data protection* is very general. All the identified strategies could be described as data protection strategies; therefore, it was not included.

Transferability

The results of this study are transferable to other industries as protection of sensitive data from hackers is important in most industries. The recent ransomware attacks on Colonial Pipeline and JBS Meat Packing have caused public panic and price increases. The results of this study could easily be applied in such industries that rely on IT systems. The results can also be applied beyond the U.S. borders, as other countries have the same issues of increasing attacks on their systems.

Replication of the study for other industries or geographical locations could be easily attained as the content and procedures are written in easy-to-understand language, and the methods used for recruiting participants are described in detail. The list of strategies from the literature review was the starting point of the first survey and these strategies could be applied in various environments. The results and replication of this study are transferrable to any company using IT.

Dependability

Audit trail information was documented and securely stored throughout the study to help ensure dependability. The raw data collected was stored in SurveyMonkey, downloaded to a secure drive, and backed up on an encrypted thumb drive. Spreadsheets capturing data reduction and analysis are also stored in the audit folder. Notes on the process, reflections, and creation of subsequent survey questions were also kept. Notes on communications with the participants were also stored during the process. Dependability strategies described in chapter 3 were followed and documented, which allowed me to include details in chapter 4 of information regarding data collection, data analysis, and results.

Confirmability

Information about the study can be confirmed as trustworthy. If this study were to be replicated, the same results could be achieved. The details of the process and each stage of the study were well documented. Specifically, during the data analysis process, I showed how I coded and then rolled codes up into themes; this information was documented in this dissertation and in the audit trail documentation. Other researchers could duplicate the process and come up with similar results.

Study Results

Round 1 Survey Results

After closing the survey for Round 1 on April 10, 2020, the data from SurveyMonkey responses (see Appendix C) was extracted and stored in a secure manner. The data was stored in a spreadsheet and analyzed. The data was then transferred into a table format (see Table 5) where scores could easily be analyzed. The nine lowest scoring items were removed from the study questions for the next round of surveys and the nine highest scoring items were carried forward. As described in the data analysis section for Round 1 above, two strategies were similar and were merged. This resulted in eight strategies, rather than nine, to be carried forward into Round 2. The list of eight was presented as the first question in Round 2 and participants ranked them according to the level of desirability, feasibility, and importance.

The summary in Table 5 below shows the results from questions 2 through 19, and also includes the question numbers, the strategy, and the number of participants who indicated the strategy is *desirable*, *feasible*, *important*, *all of the above*, or *none of the above*. The list shows nine items in normal black text and nine items in italicized text. The black text items were carried forward to Round 2. The italicized text items are the items that were not carried forward due to the lower number of responses. The column for all the above was a primary driver in the determination of which items were removed from the list.

Table 5

Round 1 Survey—Summary of Results

Question #	Strategy	Desirable	Feasible	Important	All of the above	None of the above
2	Cybersecurity Awareness and Training			11	16	
3	Strong Passwords and Multifactor Authentication			12	15	
4	Establishing a Cybersecurity Program			11	16	
5	*Culture of Risk Awareness*	*2*	*3*	*9*	*13*	
6	*Monitoring Mobile Devices and Social Media*	*4*	*7*	*3*	*9*	*4*
7	Risk Analysis and Risk Management Plans			12	15	
8	Cybersecurity Hygiene (backups, patching, etc.)			12	15	
9	*Built-in Upfront Security Mechanisms*	*5*	*5*	*7*	*9*	*1*
10	*Cyber Insurance*	*4*	*1*	*14*	*8*	
11	*3- to 5-Year Cybersecurity Plan*	*5*	*5*	*7*	*8*	*2*
12	*Asset Management (Inventory of Software and Hardware)*	*3*	*2*	*15*	*7*	
13	Continuous Monitoring of Critical Systems	1	1	12	13	
14	Incident Response Plans and Testing	1		13	13	
15	*Encryption of Data at Rest and In Transit*	*3*	*1*	*15*	*8*	
16	Intrusion Detection and Prevention Tools		1	13	13	
17	Backup and Recovery Testing	1		13	13	
18	*Recruiting, Training and Retraining Cybersecurity Staff*	*3*	*1*	*13*	*10*	
19	*Internal Stakeholder Alignment with Cybersecurity Strategies*	*1*	*4*	*11*	*11*	

Note. Nine items in italics were strategies chosen to not be carried forward in Round 2.

In addition to the strategies above from Round 1, there were 16 participants who provided responses to the open text Q20 (reference Appendix C). These responses were analyzed, consolidated, and resulted in an additional 10 questions for the next round of surveys. Participants were asked to indicate the desirability, feasibility, and importance of these added 10 strategies in Round 2. These 10 new strategies include:

1. Identity Access Management (all system accounts including vendor and privileged accounts are appropriately provisioned, deprovisioned, and regularly reviewed);
2. Governance (executive and board-level engagement, alignment to operations);
3. Cybersecurity Frameworks (i.e., NIST, HIPAA, ISO);
4. Cybersecurity Policy and Procedures (documented, regularly reviewed, and updated);
5. Third-Party Vendor Management (assessing, business associate agreements);
6. Application Management (changes, releases, testing, etc.);
7. Cloud Security;
8. Medical Device Security;
9. Data Analytics and Predictive Artificial Intelligence (AI); and
10. Data Loss Prevention (tools to stop exfiltration).

As one example where consolidation of the 16 participant’s open text comments was required was the Identity Access Management strategy. When there were similarities in the comments, they were rolled into the higher-level theme. The comments provided by three survey participants included:

- “Identity access and authorization control” (P10);
- “Identity Management, vendor account controls, privileged account controls” (P11); and
- “Restricting access to external sites (web filtering, personal email apps), multi-factor authentication for remote access, privileged account access monitoring.” (P15).

In general, identity access management includes enterprise-wide processes for requesting and authorization of access, granting access, changes to access, termination of access, and regular reviews to ensure access is appropriate. This is also sometimes referred to as provisioning and deprovisioning of accounts. Centralized access provisioning and deprovisioning, such as single sign-on (SSO), simplifies the management activities involved. Access to all information systems, including servers, databases, applications, and medical devices should be considered within this strategy.

Comments about access for vendors and privileged administrative accounts are included in two responses (P11 and P15). These are important to consider in the strategy as many breaches are found to have used vendor and administrative accounts for unauthorized access. The least privilege rule should be enforced to ensure only the access required to perform job duties is granted. Vendor and administrative accounts require additional logging and monitoring to alert support team members if nefarious activity is detected.

After the conclusion of the Round 1 survey, the responses were reviewed and analyzed, the activities were documented and securely stored, and the drafting of Round

2 survey questions was completed—all as originally planned. The goal of Round 1 was to reduce the original 18 strategies and request additional strategies that the expert participants felt were desirable, feasible, and important for cybersecurity in healthcare. The original 18 strategies were successfully reduced to eight, and 10 new strategies were added based on the open text data from the participants for Round 2 of the survey.

Round 2 Survey Results

The survey for Round 2 was closed on May 2, 2020. The data from SurveyMonkey (see Appendix E) was extracted and stored securely. Initially, the information was stored in an Excel spreadsheet and then moved to the table format as seen in Table 6.

The first question of Round 2 included the list of eight strategies identified in Round 1 and requested survey participants to rank them in order of desirability, feasibility, and importance. For the remaining questions and like Round 1, Table 6 shows the 10 new strategies uncovered in Round 1. Five areas that scored the highest are in normal text and five strategies that scored the lowest are identified in italicized text. These were not carried forward into Round 3 as desirable, feasible, and important strategies in cybersecurity for the healthcare industry.

Question one results from participants ranking the list in Round 2 are included below. The top three are the same as identified in the final Round 3 of the surveys. The study had not met saturation as there were new strategies to be considered and ranked by the participants in the final round.

1. Establishing a Cybersecurity Program

2. Strong Passwords and Multifactor Authentication
3. Cybersecurity Hygiene (backups, patching, recovery testing, etc.)
4. Risk Analysis and Risk Management Plan
5. Cybersecurity Awareness and Training
6. Continuous Monitoring of Critical Systems
7. Incident Response Plans and Testing
8. Intrusion Detection and Prevention Tools

The additional 10 strategies were included as Questions 2–11 and the results were summarized. Participants were able to check boxes and select more than one answer, unlike Round 1 where one selection of multiple-choice was allowed. Therefore, the total column was added for this round. Those that answered the *None of the Above* had their response deducted from the total column. In question 4, Cybersecurity Frameworks, the total score was 33, which was high enough to be carried into the final round; however, the number of participants indicating this was an important strategy was only 14. As a result, it was not taken forward into Round 3.

Table 6

Round 2 Survey—Summary of Results Q2 through Q11

Question #	Strategy	Desirable	Feasible	Important	None of the above	Total
2	Identity Access Management	10	12	18		40
3	Governance (Executive and board-level engagement, alignment to operations)	8	8	17		33
4	*Cybersecurity Frameworks (i.e., NIST, HIPAA, ISO)*	*9*	*10*	*14*		*33*
5	Cybersecurity Policy and Procedures (documented, regularly reviewed, and updated)	6	8	17		31
6	3rd Party Vendor Management (Assessing, Business Associate Agreements)	9	9	16		31
7	*Application Management (Changes, Releases, Testing, etc.)*	*7*	*11*	*12*	*-1*	*30*
8	Cloud Security	11	11	17		39
9	*Medical Device Security*	*10*	*7*	*15*		*32*
10	*Data Analytics and Predictive Artificial Intelligence (AI)*	*12*	*12*	*2*	*-2*	*30*
11	*Data Loss Prevention (tools to stop exfiltration)*	*10*	*7*	*15*	*-1*	*32*

Note. Five items in italicized text were strategies not carried forward to Round 3.

The final question of Round 2 asked if there was any feedback or questions for the researcher. There was only one response from P15: “All of these are important parts of a comprehensive healthcare security program and not optional items. The one exception is Data Analytics and AI, which at this point is desirable and feasible, but not required.” The first sentence is interesting as this expert indicated that none of the strategies are optional and should all be included in a comprehensive healthcare program.

Unfortunately, due to budget, personnel, and other limited resources, not everything on the list is adequately implemented in most healthcare organizations. I disagree with the second sentence about not being required. It depends on the type of data being stored for data analytics and artificial intelligence. If the data is ePHI, the HIPAA Security Rule requires the data to be adequately protected.

After appropriate analysis and conclusions, Round 2 data was used to create the questions for the final round of surveys. In the reflection notes on Round 2, I indicated the twenty responses for Round 2 came in relatively quickly and the round was closed after only fifteen days. In hindsight, Round 2 should have remained open and allowed for more time to get additional responses. This may have enabled meeting the goal of 20 responses for Round 3 surveys.

Round 3 Survey Results

The survey for Round 3 closed on June 3, 2021. Similar to rounds one and two, the data from SurveyMonkey was extracted and stored securely. The details and raw data for Round 3 are captured in Appendix G. The top three scoring strategies included the establishment of a cybersecurity program, strong passwords and multifactor authentication, and cybersecurity hygiene. The entire ranked list is shown below.

Table 7

Round 3 Survey—Summary of Results

Score	Strategy
1	Establishing a Cybersecurity Program
2	Strong Passwords and Multifactor Authentication
3	Cybersecurity Hygiene (backups, patching, recovery testing, etc.)
4	Risk Analysis and Risk Management Plan
5	Governance (executive and board-level engagement, alignment to operations)
6	Intrusion Detection and Prevention Tools
7	Incident Response Plans and Testing
8	Continuous Monitoring of Critical Systems
9	Cybersecurity Awareness and Training
10	Identity Access Management
11	Cybersecurity Policy and Procedures (documented, regularly reviewed, and updated)
12	Cloud Security 3rd Party Vendor Management (assessing, business associate agreements)

In addition to ranking the list, eight of the participants responded to the request for feedback or questions for the research (reference Appendix G). The open text area allowed participants to add comments. Out of the eight comments, two were specific to cloud computing. P5 indicated “Cloud security might be a higher priority for organizations with heavy reliance on cloud solutions.” And P3 indicated “Cloud security has an odd overlap with many of the other categories. For example, continuous monitoring of critical systems, intrusion detection, and cybersecurity hygiene would all by default include your cloud systems; true of many other categories too.” Both comments provide insight for those healthcare organizations that have taken advantage of implementing cloud solutions. Ultimately, the ePHI for their organizations must be protected, regardless of where the ePHI is created, stored, and transmitted.

Summary

The following research question guided this qualitative classical Delphi study: What are the U.S. IT healthcare cybersecurity experts' views on the desirability, feasibility, and importance of effective cybersecurity risk mitigation techniques? This research question relied on the experiences of the experts to determine the level of consensus on risk mitigation techniques. This consensus was gained by utilizing three rounds of surveys where data was collected and analyzed using SurveyMonkey. Each round provided additional data for the following round of survey questions.

In Round 1, the initial list of 18 risk mitigation techniques, developed from the literature review, was provided to the participants. The participants indicated their thoughts of desirability, feasibility, and importance for each, and 10 additional techniques were collected in the open text area. In Round 2, participants ranked the top eight strategies from Round 1 and indicated desirability, feasibility, and importance of 10 new participant-identified strategies from the Round 1 open text question.

In Round 3, participants ranked the top 12 techniques in order of desirability, feasibility, and importance. The results indicated the following top three scoring strategies were identified by the survey participants:

1. Establishing a cybersecurity program;
2. Strong passwords and multifactor authentication; and
3. Cybersecurity hygiene (backups, patching, recovery testing, etc.).

If a cybersecurity program is established and it covers the other top 11 strategies sufficiently, then the organization should be well protected. Strong passwords and multifactor authentication are two separate controls as one participant had pointed out in the final survey; however, they both deal with logging into systems and should be implemented together to reduce the likelihood of unauthorized access. Cybersecurity hygiene provides the ability to recover from backups if a ransomware attack occurs and systems are encrypted by the hackers.

In the final chapter, the interpretations of findings, the limitations and recommendations are included. The implications to social change are described; and the last section is the conclusion section where the three top scoring strategies are listed again in a concise manner.

Chapter 5: Discussion, Conclusions, and Recommendations

As previously indicated, the purpose of this qualitative classical Delphi study was to determine how a panel of 25 CISOs in U.S.-based healthcare organizations view the desirability, feasibility, and importance of IT cybersecurity risk mitigation techniques. After three rounds of surveys, the following were found to be the three top-scoring strategies:

1. Establishing a cybersecurity program;
2. Strong passwords and multifactor authentication; and
3. Cybersecurity hygiene (backups, patching, recovery testing, etc.).

This chapter contains a review of each of the three top-scoring strategies in detail and compares with the Chapter 2 literature review information on these topics. The limitations of the studies, recommendations for additional research, and implications of this research are discussed, and the conclusion section is presented.

Interpretation of Findings

The top three strategies identified by the survey participants of this study were included in the peer-reviewed literature review in Chapter 2. This study confirms the cybersecurity expert's opinions that the desirability, feasibility, and importance of the three highest-scoring strategies were also identified by multiple authors in the literature review. Each of the top three strategies is discussed in detail below including the literature review references to provide context and assist with the correct interpretation of each strategy.

Establishing a Cybersecurity Program

By establishing an appropriate cybersecurity program, the organization would include the other identified strategies from this study in the program. The cybersecurity program must be designed specifically to the organizational needs. A large organization would have many different requirements and a larger budget than a small organization. The cybersecurity program would need to consider what regulatory requirements must be met in addition to providing adequate protection to the confidentiality, integrity, and availability of the information systems.

Two participants commented that many of the strategies on the list in the survey were overlapping and need to be implemented together. From Round 3, P7 noted, “Many of these initiatives need to run in parallel to minimize risk and exposure or breach.” And in Round 3, P3 indicated that “Cloud security has an odd overlap with many of the other categories. For example, Continuous Monitoring of Critical Systems, Intrusion Detection, and Cybersecurity Hygiene would all by default be included in your cloud systems. True of many other categories too.” By establishing a cybersecurity program that considers the implementation of all these strategies, the organization will be better protected.

In the literature review, Anderson (2018) and Gibson (2020) indicated the need for establishing a cybersecurity program. The details of what a program should include differed; however, both authors agreed on the need to establish and define training for cybersecurity personnel. Recruiting, training, and retaining cybersecurity staff was not a strategy that participants in this study felt strongly about and, therefore, it was eliminated in Round 1 of the surveys (see Appendix C, R1, Q18).

According to Anderson (2018), a cybersecurity program should address procedures, personnel, and training, to provide an approach that is organized and methodical. The program should identify the hierarchy of responsibility for security roles. Anderson also indicated that there must be policies and procedures that provide employee's guidance and accountability. One comment made in Round 3 by P9 for Question 2 was that "a piece of paper does not *directly* protect the confidentiality, integrity, and availability of information systems." The comment was specific to Business Associate Agreements (BAAs); however, the comment could also apply to policy and procedures. In the HIPAA rules, there are regulatory requirements that indicate policy and required procedures. The policies and procedures must also be enforceable, so if the policies are not followed, sanctions can be applied up to and including termination of employment.

In the study conducted by Gibson (2020), the cybersecurity program was described as cybersecurity implementation. The top three key elements identified were understanding the threat landscape, establishing operational objectives and priorities, and security infrastructure and design. Other themes identified by Gibson echo Anderson (2018) to ensure personnel is provided cybersecurity training. In the cybersecurity environment, changes in the threat landscape are constant. Training is critical to stay on top of the latest trends and for establishing the right cybersecurity program for the organization.

Strong Passwords and Multifactor Authentication

Access to information systems containing ePHI must have proper authentication controls in place. Anderson (2019) and Happa et al. (2019) indicated that strong passwords and multifactor authentication are important strategies to mitigate the risk of easy access to hackers. Organizations continue to allow the use of weak passwords with complexity rules that only require eight characters and do not require upper and lower case letters, numbers, or special characters in the password. Using software to brute force these passwords allows hackers unauthorized access to systems sometimes in just minutes. Multifactor authentication normally entails sending a number to the user's designated cell phone number and requires the user to enter this number into the application before access is allowed. This provides additional protection; however, recent attacks have bypassed this multifactor authentication as well. With strong passwords and multifactor authentication, the hackers are deterred from these systems and will move on to more easily attainable targets.

Cybersecurity Hygiene

With the recent increase in ransomware attacks (i.e., Colonial Pipeline, JBS Meat Packing, Ireland's healthcare system, etc.) all organizations should be reassessing their cybersecurity hygiene processes. Copies of all information systems and databases should be created and maintained per the risk tolerance of the organization. Recovering from the copies should be conducted on a regular basis to ensure these backups are working properly. If a system is attacked and ransomware encrypts or deletes all systems and data, the organization should be able to recover its systems from backups without paying the ransom. If enough organizations can do this, then the bad actors will find it is no longer financially rewarding and will stop these types of attacks.

Applying the most recent patches will help secure systems from known vulnerabilities, especially for the older, end-of-life systems that should have been replaced and are no longer supported. Hackers target organizations that have older systems in place; they know the vulnerabilities that exist in these unpatched systems. Exploiting one vulnerability will gain the hacker access into one system, and from there, they can then move laterally from system to system during reconnaissance and find the most valuable systems and data. This activity can go on undetected for months when organizations do not have the proper logging and monitoring in place.

In summary of the interpretation of findings section, the highest-scoring strategies uncovered during this study can be implemented in varying ways from organization to organization, depending on the risk appetite and cybersecurity budget for the organization. Establishing a cybersecurity program, requiring strong passwords and multifactor authentication, and implementing good cyber hygiene can help protect organizations from being breached.

Limitations of the Study

In Chapter 1, the potential limitations were identified as limited guidance in analyzing results, generalization of results to a wider population, opinions of a small group of cybersecurity experts might not match those of a wider scope, questions being delivered via electronic survey, and personal bias. The effect of these limitations was minimized during the study, as they had been identified before the start of the study and included ways to reduce the impact. These limitations are reviewed in this section.

Analysis for this study was not difficult, but it was time consuming. The survey results were displayed as graphs by SurveyMonkey automatically and raw data were extracted from SurveyMonkey and saved in various formats for grouping, sorting, and scoring. The lack of guidance on this topic is understandable since each research study is quite different based on the topics, the instruments used, and the number of participants.

This study identified the top three cybersecurity strategies; these results might not be the same if a larger group were surveyed or if the industry was something other than healthcare. Other countries may have an emphasis on other areas of cybersecurity to mitigate cybersecurity risks and could have varying results. The study could be easily replicated in various scenarios to determine if a larger group of experts in different industries or other countries would have the same top three strategies identified.

An additional limitation initially identified was that delivering the surveys electronically could introduce communication errors. However, this method of delivery ended up being a good choice since the COVID-19 virus has stopped people from meeting face-to-face to reduce the spread of the virus. All communications between me and the respondents were conducted via LinkedIn and SurveyMonkey. There were no obvious impacts to communications due to the use of electronic communications.

The last limitation identified in Chapter 1 was potentially my personal bias. My years of experience in the IT field could have swayed the results one way or the other, but I kept them in check by reviews during the analysis phase and while writing questions for all three rounds of the survey. Judgments about the correctness of responses were minimized to the extent possible.

There were no additional limitations identified during the study and, as described above, the impact of these potential limitations was reduced by identification and consideration before the start of the study. There is a possibility this study could easily be replicated in other situations. Special consideration of limitations should be considered for all research.

Recommendations

Additional research could be conducted to replicate this study in various scenarios such as surveying a larger group of CISOs, other industries besides healthcare could be surveyed, and the study could be conducted outside of the United States. IT is used in almost all industries across the globe, making these industries more susceptible to cybersecurity attacks. It would be beneficial for organizations to study cybersecurity strategies. This would help to ensure the right strategies are applicable and will mitigate the risk of breaches specific to their organizations.

The initial questions for the first survey were based on information synthesized from the literature review in Chapter 2. To duplicate a similar study using the instrumentation developed for this survey would be straightforward. If the results of the survey differ, which is likely, the questions for Rounds 2 and 3 will need to be adjusted accordingly. Utilizing an already developed instrument could save the researcher many hours of effort. A larger number of participants could be surveyed to see if the results are similar. Gathering more opinions could reveal more accurate results. According to Avella

(2016), the Delphi method can include an acceptable range of participants (10 to 100). There is no agreed-upon standard.

Targeting CISO-level individuals as participants in the survey would ensure that broader perspectives would be captured and not just expertise in one specific area (i.e., network security, access management, application development security, etc.). It would be recommended to survey those in decision-making positions as they have a wealth of knowledge. As seen in this study, CISOs are willing to share their knowledge to help advance the field.

This study could be replicated in other industries as long as they are utilizing IT systems. We recently saw a gas company (i.e., Colonial Pipeline) and a meatpacking company (i.e., JBS) forced to pay millions in ransom to get their systems back online. The public saw increases in gas and meat prices during the uncertain times immediately following the attack. The impacts could have been worse, where the loss of life could occur. Other industries are not as targeted by hackers as much as the healthcare industry for a variety of reasons as discussed in Chapter 2. See Figure 4 to review the list of other industries and compare average costs of breaches. More and more attacks are occurring across all industries every day, and as long as the hackers continue to make money and go undetected, this growth will continue.

Other countries could find similar results if they were to survey their healthcare CISOs for large healthcare organizations. Healthcare systems across the globe are using EMRs, making them susceptible to attacks. Other regulations may be in place and could affect the outcomes; however, all cybersecurity strategies could apply to other countries, regardless of the laws in place. Translation of the survey questions into the language of the country could be done using translations tools.

This section included various recommendations for how this study could be replicated. The number of people involved, the industry, and other countries could all be variables that change to conduct similar studies to determine the best mitigation strategies. It is time to join forces against the hackers and learn from each other on how to stop them.

Implications

The potential impact of this study for positive social change, in general, includes increasing the ability to use healthcare technology in a secure and safe manner. This could result in increasing accessibility of healthcare for underserved populations. By reducing successful cybercrime attacks, costs related to the attacks would be reduced and patient trust in healthcare organizations would increase. Each of these four items is discussed further in the following paragraphs.

Increasing Ability to Use Technology in a Secure and Safe Manner

As healthcare organizations continue to improve the maturity of their cybersecurity programs and implement recommended strategies from this study, the public could have increased confidence when using healthcare systems that their data is adequately and properly protected. This increased confidence can allow patients greater usage of technology for meeting day-to-day medical needs. This could result in expanding the use of technology for areas needing better access to healthcare.

Increasing Accessibility of Healthcare for Underserved Populations

By improving defenses against cybersecurity attacks, the capability for secure healthcare can be expanded. We witnessed a dramatic growth in telehealth visits during the COVID-19 pandemic; telehealth has provided the ability to receive medical care without ever stepping foot in a doctor’s office. The security safeguards put into place in the past years has allowed this exchange of information to occur in a secure manner. The implications of further expanding telehealth visits are exciting and could bring secure healthcare to remote rural areas that have not had adequate medical coverage available in the past.

Reducing Costs of Cyberattacks

This study could help reduce the costs of healthcare breaches. By reducing the number of successful cyberattacks, healthcare organizations could save millions. In 2018, the cost estimate of a healthcare data breach was $2.2 million (Lee et al., 2018). The average cost of a healthcare breach in 2019 was $3.92 million, and for 2020 it was $7.1 million (Ponemon, 2019, 2020). If the trend continues to double each year, we could see the average in 2021 grow to $14 million. Many healthcare organizations might not survive the financial loss. The savings from implementing the strategies identified in this study could be used for providing better care to their patients.

Increase Patient Trust in Healthcare

Organizations that adequately protect patient data by implementing the strategies provided in this study will have continued levels of patient trust. Reputational risk is difficult to quantify; however, Choi and Johnson (2019) found breaches in hospitals were associated with a decrease in outpatient visits and admissions. For those organizations that continue to be affected by cyberattacks, their patients will seek out other healthcare providers. If the organization cannot protect patient data, the patient will not trust the organization with their health.

Conclusions

The CISO cybersecurity experts for large U.S.-based healthcare organizations indicated the top three high scoring desirable, feasible, and important cybersecurity strategies:

1. Establishing a cybersecurity program;
2. Strong passwords and multifactor authentication; and
3. Cybersecurity hygiene (backups, patching, recovery testing, etc.).

These strategies, if implemented appropriately, will help mitigate cybersecurity risks and reduce the probability and impact of cyberattacks.

References

Aaltola, K., & Taitto, P. (2019). Utilising experiential and organizational learning theories to improve human performance in cyber training. *Information & Security*, *43*, 123–133. https://doi.org/10.11610/isij.4311

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

Ahmed, H. I., Nasr, A. A., Abdel-Mageid, S., & Aslan, H. K. (2019). A survey of IoT security threats and defenses. *International Journal of Advanced Computer Research*, *9*(45), 325–350. https://doi.org/10.19101/IJACR.2019.940088

Akhtar, U., Lee, J. W., Muhammad Bilal, H. S., Ali, T., Khan, W. A., & Lee, S. (2020). The impact of big data in healthcare analytics. 2020 *International Conference on Information Networking (ICOIN)*, 61–63. https://doi.org/10.1109/ICOIN48656.2020.9016588

Al-Saqqa, S., Sawalha, S., & AbdelNabi, H. (2020). Agile software development: Methodologies and trends. *International Journal of Interactive Mobile Technologies*, *14*(11), 246–270. https://doi.org/10.3991/ijim.v14i11.13269

Aliyu, A., Maglaras, L., He, Y., Yevseyeva, I., Boiten, E., Cook, A., & Janicke, H. (2020). A holistic cybersecurity maturity assessment framework for higher education institutions in the United Kingdom. *Applied Sciences*, *10*(3660). https://doi.org/10.3390/app10103660

Amin, M. E. K., Nørgaard, L. S., Cavaco, A. M., Witry, M. J., Hillman, L., Cernasev, A.,

& Desselle, S. P. (2020). Establishing trustworthiness and authenticity in qualitative pharmacy research. *Research in Social & Administrative Pharmacy*, *16*(10), 1472–1482. https://doi.org/10.1016/j.sapharm.2020.02.005

Anderson, Jr., R. E. (2018). Low-cost strategies to strengthen cybersecurity: Low-cost strategies can help healthcare organizations avoid the high price of a data breach. *Healthcare Financial Management*, *72*, 60+. https://www.hfma.org/topics/hfm/2018/march/59656.html

Atluri, I. (2018). Smarter cyber risk governance for health care in a digital transformation age. *ISSA Journal*, *16*, 27–31. https://mydigitalpublication.com/publication/?m=1336&i=517151&p=26

Avella, J. R. (2016). Delphi panels: Research design, procedures, advantages, and challenges. *International Journal of Doctoral Studies*, *11*, 305–321. https://doi.org/10.28945/3561

Azab, A., & Khasawneh, M. (2020). MSIC: Malware spectrogram image classification. *IEEE Access*, *8*, 102007–102021. https://doi.org/10.1109/ACCESS.2020.2999320

Azeez, N. A., & der Vyver, C. V. (2019). Security and privacy issues in e-health cloud-based systems: A comprehensive content analysis. *Egyptian Informatics Journal*, *20*, 97–108. https://doi.org/10.1016/j.eij.2018.12.001

Bajric, S. (2020, March 30). Data security and privacy issues in healthcare. *Applied Medical Informatics Research Letters*, *42*(1) 19–27. https://ami.info.umfcluj.ro/index.php/AMI/article/view/702/699

Bakertilly. (2016, January 26). *Cybersecurity management: Implementing cybersecurity* *controls*. https://www.bakertilly.com/insights/cybersecurity-management-implementing-cybersecurity-controls/

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

Barosy, W. (2019). *Successful operational cyber security strategies for small businesses* (Publication No. 13898243) [Doctoral study, Walden University]. ProQuest Dissertations and Theses Global.

Birkinshaw, C., Rouka, E., & Vassilakis, V. G. (2019). Implementing an intrusion detection and prevention system using software-defined networking: Defending against port-scanning and denial-of-service attacks. *Journal of Network & Computer Applications, 136*, 71–85. https://doi.org/10.1016/j.jnca.2019.03.005

Botelho, J. (2017). How automating data collection can improve cyber-security. *Network Security, 2017*(6), 11–13. https://doi.org/10.1016/S1353-4858(17)30061-2

Brady, S. R. (2016). The Delphi method. In L. A. Jason & D. S. Glenwick (Eds.). *Handbook of methodological approaches to community-based research: Qualitative, quantitative, and mixed methods* (pp. 61–67). Oxford University Press.

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), 15–27. https://doi.org/http://doi.org/10.31646/gbio.7

Bullard, E. (2020). Meaningful use. *Salem press encyclopedia*.

Burdorf, A., Porru, F. & Rugulies, R. (2021). The COVID-19 pandemic: One year later – an occupational perspective. *Scandinavian Journal of Work, Environment & Health*, *47*(4), 245–247. https://doi.org/10.5271/sjweh.3956

Caruso, J. P., Swartz, K., Mazzola, C., Ban, V. S., Singh, R., Eldridge, C., Schirmer, C., Cheng, J., Bauer, A. M., Steinmetz, M., & Adogwa, O. (2021). The financial impact of the COVID-19 pandemic on neurosurgery practice in spring 2020. *World Neurosurgery*, *153*, e1–e10. https://doi.org/10.1016/j.wneu.2021.04.120

Castro, D. (2018). Boosting the cyber workforce: Amid persistent shortages in cybersecurity positions, what can states do to strengthen their numbers? *Government Technology, 31*(3), 48. https://www.govtech.com/data/Boosting-the-Cyberworkforce.html

Chambers, M., Bliss, K., & Rambur, B. (2020). Recruiting research participants via traditional snowball vs Facebook advertisements and a website. *Western Journal of Nursing Research*, *42*(10), 846–851. https://doi.org/10.1177/0193945920904445

Choi, S. J. & Johnson, M. E. (2019). Understanding the Relationship Between Data Breaches and Hospital Advertising Expenditures. *American Journal of Managed Care*, *25*(1), e14–e20. https://doi.org/10.1093/jamia/ocab142

Chung, C. J., Biddix, J. P., & Park, H. W. (2020). Using digital technology to address confirmability and scalability in thematic analysis of participant-provided data. *Qualitative Report*, *25*(9), 3298–3311. https://doi.org/10.46743/2160-

3715/2020.4046

Colicchio, T. K., Cimino, J. J., & Del Fiol, G. (2019). Unintended consequences of nationwide electronic health record adoption: Challenges and opportunities in the post-meaningful use era. *Journal of Medical Internet Research, 21*(6). https://doi.org/10.2196/13313

Compliancy Group. (2020). *HIPAA electronic protected health information (ePHI).* https://compliancy-group.com/hipaa-ephi-electronic-protected-health-information/

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

Cook, K. D. (2017). *Effective cyber security strategies for small businesses*. https://www.semanticscholar.org/paper/Effective-Cyber-Security-Strategies-for-Small-Cook/00916ef24863c548656bf1150daa828a1408ef5e

Cope, R. (2020). Strong security starts with software development. *Network Security, 2020*(7), 6–9. https://doi.org/10.1016/S1353-4858(20)30078-7

Coventry, L., & Branley, D. (2018). Cybersecurity in healthcare: A narrative review of trends, threats, and ways forward. *Maturitas, 113*, 48–52. https://doi.org/10.1016/j.maturitas.2018.04.008

Creswell, J. W. & Creswell, J. D. (2018). *Research design: Qualitative, quantitative, and mixed methods approaches.* SAGE Publications.

Cronin, C. (2020). What lawyers mean by 'reasonable' cyber security controls. *Cyber*

Security: A Peer-Reviewed Journal, *3*, 315–329. https://www.ingentaconnect.com/content/hsp/jcs/2020/00000003/00000004/art00004

Cybersecurity Market Report (2018). *Cybersecurity ventures*. http://cybersecurityventures.com/cybersecurity-market-report/

Cybersecurity Ventures (2020). *Cybercrime to cost the world $10.5 trillion annually by 2025. Special Report: Cyberwarfare in the C-Suite*. https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/

Dameff, C., Pfeffer, M. A., & Longhurst, C. A. (2019). Cybersecurity implications for hospital quality. *Health Services Research*, *54*(5), 969–970. https://doi.org/10.1111/1475-6773.13202

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), 118–129. https://doi.org/10.34190/JBRM.17.3.002

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

DeWitt, M. (2018). *CDC data shows U.S. life expectancy continues to decline: Suicide, drug overdose named as key contributors*. https://www.aafp.org/news/health-of-the-public/20181210lifeexpectdrop.html

Fischer, B., Gral, B., & Lehner, O. (2020). SOX section 404 twenty years after: Reviewing costs and benefits. *ACRN Journal of Finance and Risk Perspectives*, *9*(1), 103–112. https://doi.org/10.35944/jofrp.2020.9.1.008

Gibson, G. (2020). *A comprehensive strategy for cybersecurity implementation within the department of defense: A Delphi study*. https://www.proquest.com/openview/cdc6908b80ed4e795f6c6e92551012bb/1?pq-origsite=gscholar&cbl=18750&diss=y

Gonen, B., & Sawant, D. (2020). Significance of agile software development and SQA powered by automation. *2020 3rd International Conference on Information and Computer Technologies (ICICT),* 7–11. https://doi.org/10.1109/ICICT50521.2020.00009

Greene, J. M. (2020). Ransomware. *Salem Press Encyclopedia of Science.*

Happa, J., Glencross, M., & Steed, A. (2019). Cyber security threats and challenges in collaborative mixed-reality. *Frontiers in ICT*. https://doi.org/10.3389/fict.2019.00005

Hausfeld, J., & Zimmerman, R. (2018). Your organization can and should be cyber secure. *The Journal of Medical Practice Management, 33*(6), 389–391. https://www.proquest.com/openview/ffe7397237d815ea98d0126e3029afd7/1?pq-origsite=gscholar&cbl=32264

Henriques de Gusmão, A. P., Silva, M. M., Poleto, T., Camara e Silva, L., & Cabral Seixas Costa, A. P. (2018). Cybersecurity risk analysis model using fault tree analysis and fuzzy decision theory. *International Journal of Information Management*, *43*, 248–260. https://doi.org/10.1016/j.ijinfomgt.2018.08.008

Hintze, M. (2018). Data controllers, data processors, and the growing use of connected products in the Enterprise: Managing risks, understanding benefits, and complying with the GDPR. *Journal of Internet Law, 22*(2), 17–31. https://doi.org/10.2139/ssrn.3192721

Hoffman, S. (2020). Cybersecurity threats in healthcare organizations: Exposing vulnerabilities in the healthcare information infrastructure. *World Libraries, 24.* http://worldlibraries.dom.edu/index.php/worldlib/article/view/588/678

Ibarra, J., Jahankhani H., & Kendzierskyj, S. (2019). Cyber-physical attacks and the value of healthcare data: Facing an era of cyber extortion and organised crime. In H. Jahankhani, S. Kendzierskyj, A. Jamal, G. Epiphaniou, & H. Al-Khateeb (Eds). *Blockchain and clinical trials. Advanced sciences and technologies for security applications*. Springer, Cham. https://doi.org/10.1007/978-3-030-11289-9_5

Isabelle, D., Horak, K., McKinnon, S., & Palumbo, C. (2020). Is Porter's five forces framework still relevant? A study of the capital/labour intensity continuum via mining and IT industries. *Technology Innovation Management Review, 10*(6), 28–41. https://doi.org/10.22215/timreview/1366

Jalali, M. S., Bruckes, M., Westmattelmann, D., & Schewe, G. (2020). Why employees (still) click on phishing links: Investigation in hospitals. *Journal of Medical Internet Research, 22*(1). https://doi.org/10.2196/16775

Jalali, M. S., & Kaiser, J. P. (2018). Cybersecurity in hospitals: A systematic, organizational perspective. *Journal of Medical Internet Research, 20*(5). https://doi.org/10.2196/10059/

Jalali, M. S., Razak, S., Gordon, W., Perakslis, E., & Madnick, S. (2019). Health care and cybersecurity: Bibliometric analysis of the literature. *Journal of Medicine Internet Research, 21*(2). https://doi.org/10.2196/jmir.12644

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), 138–146. https://doi.org/10.5688/ajpe7120

Joint Task Force Transformation Initiative. (2015, January 22) *NIST 800-53, security and privacy controls for federal information systems and organizations*. https://doi.org/10.6028/NIST.SP.800-53r4

Kalso, R. (2020). Waterfall model. *Salem Press Encyclopedia of Science.*

Kamiya, S., Kang, J.-K., Kim, J., Milidonis, A., & Stulz, R. M. (2019). Risk management, firm reputation, and the impact of successful cyberattacks on target firms. *Journal of Financial Economics*. https://doi.org/10.1016/j.jfineco.2019.05.019

Kaušpadienė, L., Ramanauskaitė, S. & Čenys, A. (2019). Information security management framework suitability estimation for small and medium enterprise. *Technological and Economic Development of Economy*. https://doi.org10.3846/tede.2019.10298

Keshta, I. & Odeh, A. (2020). Security and privacy of electronic health records: Concerns and challenges. *Egyptian Informatics Journal.* https://doi.org/10.1016/j.eij.2020.07.003

Kolb, A., & Kolb, D. (2009). “Experiential learning theory: A dynamic, holistic approach to management learning, education and development." In S. J. Armstrong & C. V. Fukami (Eds.), *The SAGE handbook of management learning, education, and development*. Sage. https://doi.org/10.4135/9780857021038.n3

Kopel, J., Hier, D., & Thomas, P. (2019). Electronic health records: Is mindfulness the solution? *Baylor University Medical Center. Proceedings*, *32*(3), 459–461. https://doi.org/10.1080/08998280.2019.1588839

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

Kruse, C. S., & Beane, A. (2018). Health information technology continues to show positive effect on medical outcomes: Systematic review. *Journal of Medical Internet Research, 20*(2), e41. https://doi.org/10.2196/jmir.8793

Kruse, C. S., Frederick, B., Jacobson, T., & Monticone, D. K. (2017). Cybersecurity in healthcare: A systematic review of modern threats and trends. *Technology and Health Care: Official Journal of the European Society for Engineering and Medicine*, *25*(1), 1–10. https://doi.org/10.3233/THC-161263

Langer, S. G. (2017). Cyber-security issues in healthcare information technology. *Journal of Digital Imaging, 30*(1), 117-125. https://doi.org/10.1007/s10278-016-9913-x

Larson, S., Jones, J., & Swauger, J. (2019). A forensic first look at a POS device: Searching for PCI DSS data storage violations. *Proceedings of the Conference on Digital Forensics, Security & Law*, 1–15.

https://doi.org/10.15394/jdfsl.2020.1614

Lee, E., Daugherty, J., & Hamelin, T. (2018). Reimagine health care leadership, challenges and opportunities in the 21st century. *Journal of PeriAnesthesia* Nursing. https://doi.org/10.1016/j.jopan.2017.11.007

Lemon, L. L., & Hayes, J. (2020). Enhancing trustworthiness of qualitative findings: Using leximancer for qualitative data analysis triangulation. *The Qualitative Report*, *25*(3), 604–14. https://doi.org/10.46743/2160-3715/2020.4222

Liu, J., Xiao, Y., Chen, H., Ozdemir, S., Dodle, S., & Singh, V. (2010). A survey of payment card industry data security standard. IEEE *Communications Surveys & Tutorials, Communications Surveys & Tutorials*, *12*(3), 287–303. https://doi.org/10.1109/SURV.2010.031810.00083

Lo, F. Y., Rey-Martí, A., & Botella-Carrubi, D. (2020). Research methods in business: Quantitative and qualitative comparative analysis. *Journal of Business Research, 115*, 221–224. https://doi.org/10.1016/j.jbusres.2020.05.003

Mallik, A., Ahsan, A., Shahadat, M., & Tsou, J., (2019). Man-in-the-middle-attack: Understanding in simple words. *International Journal of Data and Network Science*, (2), 77. https://doi.org/10.5267/j.ijdns.2019.1.001

McMahon, M. (2020). *What are detective controls*? https://www.wisegeek.com/what-are-detective-controls.htm

Meisner, M. (2018). Financial consequences of cyberattacks leading to data breaches in the healthcare sector. *Copernican Journal of Finance & Accounting, 6*(3), 63–73. http://dx.doi.org/10.12775/CJFA.2017.017

Meng, W., Li, W., Wang, Y., & Au, M. H. (2018). Detecting insider attacks in medical cyber–physical networks based on behavioral profiling. *Future Generation Computer Systems*. https://doi.org/10.1016/j.future.2018.06.007

Morgan, M. G., Zacharias, E. G., & Doddi, D. (2020). Significant increase in ransomware attacks on healthcare industry; OCR offers guidance. *Computer & Internet Lawyer, 37*(6), 3–5. https://www.mwe.com/insights/significant-increase-in-ransomware-attacks-on-healthcare-industry-ocr-offers-guidance/

Mustafa, U., Pflugel, E., & Philip, N. (2019). A novel privacy framework for secure M-health applications: The case of the GDPR. *2019 IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3),* 1–9. https://doi.org/10.1109/ICGS3.2019.8688019

National Institute of Standards and Technology (2020, January 16). *NIST 800-53.* https://www.nist.gov/privacy-framework/nist-sp-800-53

Negash, S., Musa, P., Vogel, D., & Sahay, S. (2018). Healthcare information technology for development: improvements in people's lives through innovations in the uses of technologies. *Information Technology for Development, 24*(2), 189–197. https://doi.org/10.1080/02681102.2018.1422477

Niakanlahiji, A., & Jafarian, J. H. (2019). WebMTD: Defeating cross-site scripting attacks using moving target defense. *Security & Communication Networks*, 1–13. https://doi.org/10.1155/2019/2156906

Öbrand, L., Holmström, J., & Newman, M. (2018). Navigating Rumsfeld's quadrants: A performative perspective on IT risk management. *Technology in Society, 531*.

https://doi.org/10.1016/j.techsoc.2017.09.009

Peterson, D. C., Adams, A., Sanders, S. & Sanford, B. (2018). Assessing and addressing threats and risks to cybersecurity. *Frontiers of Health Services Management, 35*(1), 23–19. https://doi.org/10.1097/HAP.0000000000000040

Pointer, P. (2020). The rise of telemedicine: How to mitigate potential fraud. *Computer Fraud & Security*, *2020*, 6–8. https://doi.org/10.1016/S1361-3723(20)30061-0

Ponemon Institute (2017). *2017 Cost of data breach study: Global overview*. https://www.ibm.com/downloads/cas/ZYKLN2E3

Ponemon Institute (2018). *2018 Cost of a data breach study: Global overview*. https://www.ibm.com/downloads/cas/861MNWN2

Ponemon Institute (2019). *The cost of cybercrime*. https://accntu.re/2HbVmgn

Ponemon Institute (2020). *Cost of a data breach report 2020.* https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/pdf

PR Newswire. (2019, November 4). Healthcare data breaches costs industry $4 billion by year's end, 2020 will be worse reports new Black Book Survey. *PR Newswire US.* https://www.prnewswire.com/news-releases/healthcare-data-breaches-costs-industry-4-billion-by-years-end-2020-will-be-worse-reports-new-black-book-survey-300950388.html

Radziwill, N., & Benton, M. (2017). Cybersecurity cost of quality: Managing the costs of cybersecurity risk management. *Software Quality Professional*, *19*, 25. https://arxiv.org/ftp/arxiv/papers/1707/1707.02653.pdf

Rayens, M.K., & Hahn, E.J. (2000). Building consensus using the policy Delphi method.

Policy, Politics & Nursing Practice, 1(4), 308–315. https://doi.org/10.1177/152715440000100409

Ripp, J., Peccoralo, L., & Charney, D. (2020). Attending to the emotional well-being of the health care workforce in a New York City health system during the COVID-19 pandemic. *Academic Medicine, 95*(8), 1136–1139. https://doi.org/10.1097/acm.0000000000003414

Roy, P. P. (2020). A high-level comparison between the NIST cyber security framework and the ISO 27001 information security standard. *2020 National Conference on Emerging Trends on Sustainable Technology and Engineering Applications (NCETSTEA)*, 1–3. https://doi.org/10.1109/NCETSTEA48365.2020.9119914

Royce, W. W (1987). Managing the development of large software systems. *Software Engineering*, 328–338. https://dl.acm.org/doi/10.5555/41765.41801

Samuels, M. (2020, March 2). *What is a CISO? Everything you need to know about the chief information security officer role*. https://www.zdnet.com/article/what-is-a-ciso-everything-you-need-to-know-about-the-chief-information-security-officer/

Schmeelk, S. (2020). Creating a standardized risk assessment framework library for healthcare information technology. *Hawaii International Conference on System Sciences*, 3881–3890. https://scholarspace.manoa.hawaii.edu/bitstream/10125/64216/0384.pdf

Schroeder, P. (2019). Healthcare quality improvement: Then and now. *Nursing Management*, *50*(9), 20–25. https://doi.org/10.1097/01.NUMA.0000579004.87116.35

Selig, G. J. (2018). IT governance—an integrated framework and roadmap: How to plan, deploy and sustain for competitive advantage. 2018 Portland International Conference on Management of Engineering and Technology (PICMET), Honolulu, HI, 2018, pp. 1–15. https://doi.org/10.23919/PICMET.2018.8481957

Sivagnanam, M. (2018). Security measures that help reduce the cost of a data breach. *ISSA Journal*, *16*(10), 31–38.

Sorace, J., Wong, H.-H., DeLeire, T., Xu, D., Handler, S., Garcia, B., & MaCurdy, T. (2020). Quantifying the competitiveness of the electronic health record market and its implications for interoperability. *International Journal of Medical Informatics*, 136. https://doi.org/10.1016/j.ijmedinf.2019.104037

Stacy, R. N. (2019). Electronic health record (EHR). *Salem Press Encyclopedia*.

Stern, G. (2018). A life cycle approach to medical device cybersecurity. *Biomedical Instrumentation & Technology*, *52*(6), 464–466. https://doi.org/10.2345/0899-8205-52.6.464

Sumit, M., & Deen, M. J. (2019). Smartphone sensors for health monitoring and diagnosis. *Sensors*, *19*(9), 2164. https://doi.org/10.3390/s19092164

Tao, H., Bhuiyan, M. Z. A., Rahman, M. A., Wang, G., Wang, T., Ahmed, M. M., & Li, J. (2019). Economic perspective analysis of protecting big data security and privacy. *Future Generation Computer Systems, 98,* 660-671. https://doi.org/10.1016/j.future.2019.03.042

Tariq, M. I., Tayyaba, S., Ashraf, M. W., Rasheed, H., & Khan, F. (2018). Risk based NIST effectiveness analysis for cloud security. *Bahria University Journal of*

Information & Communication Technology, 10, 1. https://www.researchgate.net/publication/326414860_Risk_Based_NIST_Effectiveness_Analysis_for_Cloud_Security

Techapanupreed, C., & Kurutach, W. (2020). Enhancing transaction security for handling accountability in electronic health records. *Security & Communication Networks*, 1–18. https://doi.org/10.1155/2020/8899409

Tutelman, P., & Webster, F. (2020). Qualitative research and pain: Current controversies and future directions. *Canadian Journal of Pain, 0*. https://doi.org/10.1080/24740527.2020.1809201

Tyson, B. (2017). *World economic forum center for the fourth industrial revolution*. Video. https://www.weforum.org/focus/the-fourth-industrial-revolution

Tyson, B. (2019). *Becker's hospital review*. https://www.beckershospitalreview.com/hospital-management-administration/5-thoughts-from-kaiser-permanente-ceo-bernard-tyson-on-the-future-of-us-healthcare.html

U.S. Department of Health and Human Services, Office of Civil Rights. (2013, July 26). *HIPAA security*. https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html

U.S. Department of Health and Human Services, Office of Civil Rights. (2020, August 31). *HIPAA privacy*. https://www.hhs.gov/hipaa/for-professionals/privacy/index.html

U.S. Department of Justice. (2021, March 31). *Justice Department Warns About Fake Post-Vaccine Survey Scams*. https://www.justice.gov/opa/pr/justice-department-warns-about-fake-post-vaccine-survey-scams

Vaduva, J., Pasca, V. R., Florea, I., & Rughinis, R. (2019). Applications of machine learning in malware detection. *ELearning & Software for Education, 2*, 286–293. https://doi.org/10.12753/2066-026X-19-110

Vakulyk, O., Petrenko, P., Kuzmenko, I., Pochtovyi, M., & Orlovskyi, R. (2020). Cybersecurity as a component of the national security of the state. *Journal of Security & Sustainability Issues, 9*, 775–784. https://doi.org/10.9770/jssi.2020.9.3(4)

van Veen, E.B. (2018). Observational health research in Europe: Understanding the general data protection regulation and underlying debate. *European Journal of Cancer, 104*, 70–80. https://doi.org/10.1016/j.ejca.2018.09.032

Vincent, A. (2019). Don't feed the phish: How to avoid phishing attacks. *Network Security, 2019*(2), 11–14. https://doi.org/10.1016/S1353-4858(19)30022-4

Volkova, M., Chmelar, P., & Sobotka, L. (2019). Machine learning blunts the needle of advanced SQL injections. *Mendel*, (1), 23. https://doi.org/10.13164/mendel.2019.1.023

What Will Improve Cyber Talent Retention? (2018). *Security: Solutions for Enterprise Security Leaders, 55*(4), 14. https://www.securitymagazine.com/articles/88833-what-will-improve-cyber-talent-retention

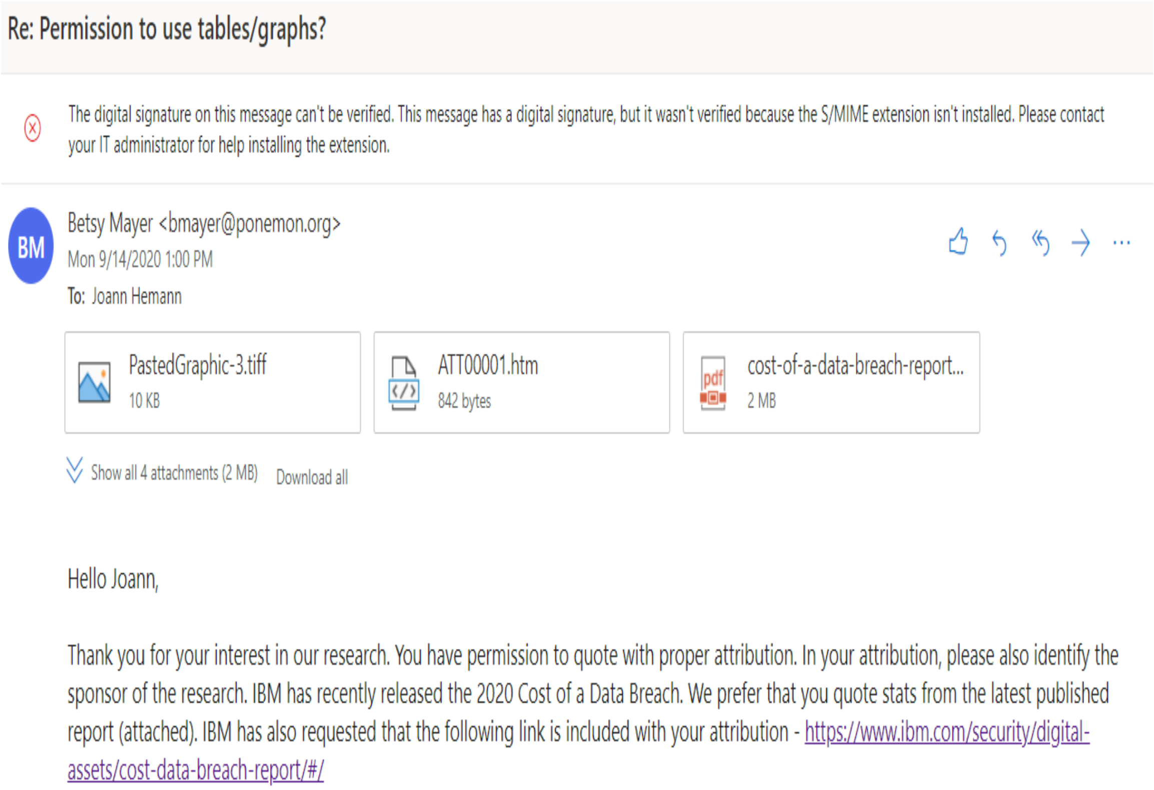
White, M. G. (2020). Why human subjects research protection is important. *Ochsner Journal, 20*(1), 16. https://doi.org/10.31486/toj.20.5012

Wosik, J., Fudim, M., Cameron, B., Gellad, Z. F., Cho, A., Phinney, D., Curtis, S., Roman, M., Poon, E. G., Ferranti, J., Katz, J. N., & Tcheng, J. (2020). Telehealth transformation: COVID-19 and the rise of virtual care. *Journal of the American Medical Informatics Association: JAMIA*, 27, 957–962. https://doi.org/10.1093/jamia/ocaa067

Yan, M., Qu, T., Li, C., & Xu, S. (2018). Impacts of health information technology on health care quality in hospital-related settings: A systematic review. *2018 IEEE 15th International Conference on Networking, Sensing and Control (ICNSC)*, 1–4. https://doi.org/10.1109/ICNSC.2018.8361316

Yun, H., Lee, G., & Kim, D. J. (2019). A chronological review of empirical research on personal information privacy concerns: An analysis of contexts and research constructs. *Information & Management*, *56*(4), 570–601. https://doi.org/10.1016/j.im.2018.10.001

Appendix A: Permission to use Ponemon Institute Sources



Re: Permission to use tables/graphs?

The digital signature on this message can't be verified. This message has a digital signature, but it wasn't verified because the S/MIME extension isn't installed. Please contact your IT administrator for help installing the extension.

Betsy Mayer <bmayer@ponemon.org>
Mon 9/14/2020 1:00 PM
To: Joann Hemann

Hello Joann,

Thank you for your interest in our research. You have permission to quote with proper attribution. In your attribution, please also identify the sponsor of the research. IBM has recently released the 2020 Cost of a Data Breach. We prefer that you quote stats from the latest published report (attached). IBM has also requested that the following link is included with your attribution - https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/

Appendix B: Round 1 Survey Questions

(Note: The first page of this survey was the consent form.)

Confirmation of Qualification Criteria

1. Please indicate the number of years you have spent as a CISO in a large U.S.-based healthcare organization with over $50M in annual revenue:

   A. None

   B. 1 - 3 years

   C. 3 – 5 years

   D. 5 – 10 years

   E. 10+ years

Note: For the next 19 questions, *desirable*, *feasible,* and *important* have the following meaning:

Desirable: something that is wanted.

Feasible: something that is possible.

Important: something that must be done.

2. Do you consider cybersecurity awareness training for employees as:

   A. Desirable

   B. Feasible

   C. Important

   D. All the above

   E. None of the above

3. Do you consider strong passwords and multifactor authentication as:

   A. Desirable

B. Feasible

C. Important

D. All the above

E. None of the above

4. Do you consider establishing a cybersecurity program as:

A. Desirable

B. Feasible

C. Important

D. All the above

E. None of the above

5. Do you consider creating a culture of risk awareness in your organization as:

A. Desirable

B. Feasible

C. Important

D. All the above

E. None of the above

6. Do you consider monitoring mobile devices and social media as:

A. Desirable

B. Feasible

C. Important

D. All the above

E. None of the above

7. Do you consider cybersecurity risk assessments and risk management plans as:

   A. Desirable

   B. Feasible

   C. Important

   D. All the above

   E. None of the above

8. Do you consider good cyber-hygiene (backups, patching, etc.) as:

   A. Desirable

   B. Feasible

   C. Important

   D. All the above

   E. None of the above

9. Do you consider upfront built-in security mechanisms as:

   A. Desirable

   B. Feasible

   C. Important

   D. All the above

   E. None of the above

10. Do you consider cyber insurance as:

    A. Desirable

    B. Feasible

    C. Important

D. All the above

E. None of the above

11. Do you consider a 3-5 year cybersecurity plan as:

A. Desirable

B. Feasible

C. Important

D. All the above

E. None of the above

12. Do you consider asset management (i.e. inventory of hardware/software) as:

A. Desirable

B. Feasible

C. Important

D. All the above

E. None of the above

13. Do you consider continuous monitoring of critical systems as:

A. Desirable

B. Feasible

C. Important

D. All the above

E. None of the above

14. Do you consider incident response plans and testing as:

A. Desirable

B. Feasible

C. Important

D. All the above

E. None of the above

15. Do you consider encryption of data at rest and in transit as:

A. Desirable

B. Feasible

C. Important

D. All the above

E. None of the above

16. Do you consider intrusion detection and intrusion prevention tools as:

A. Desirable

B. Feasible

C. Important

D. All the above

E. None of the above

17. Do you consider backup and recovery testing as:

A. Desirable

B. Feasible

C. Important

D. All the above

E. None of the above

18. Do you consider recruiting, training, and retaining cybersecurity staff as:

    A. Desirable

    B. Feasible

    C. Important

    D. All the above

    E. None of the above

19. Do you consider internal stakeholder alignment with cybersecurity priorities as:

    A. Desirable

    B. Feasible

    C. Important

    D. All the above

    E. None of the above

20. Open-ended question:

    ▪ What additional cybersecurity risk mitigation strategies are desirable, feasible, and important in your perspective that is not included in the list above?

Appendix C: Round 1 Survey Responses

At the beginning of the survey, the terms desirable, feasible, and important were described to the participants to have the following meaning:

Desirable: something that is wanted.

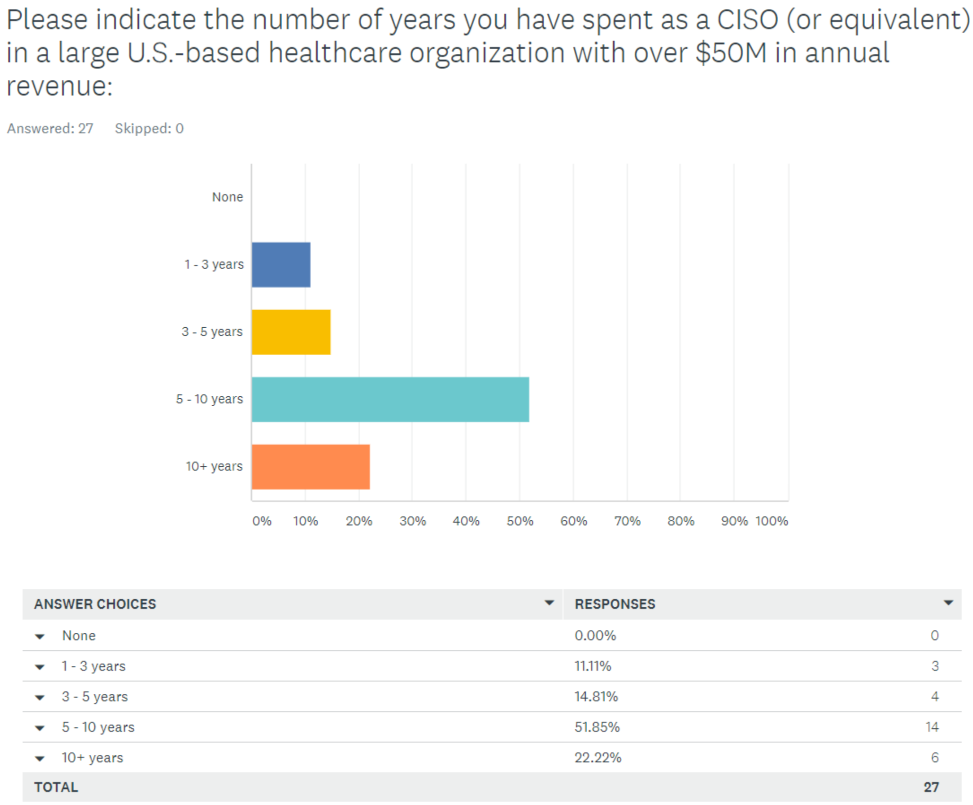
Feasible: something that is possible.

Important: something that must be done.

R1 Q1: This question was included to show the number of years of experience the participants had as a CISO in a healthcare organization. Prior to sending the survey to the recruits, the LinkedIn profiles were reviewed to ensure that the potential participants had at least 10 years of CISO experience, however, not all 10 years were required to be in healthcare organizations. Skills needed for CISOs are easily transferrable across different industries. The healthcare organizations that each recruit was employed by was also vetted, ensuring they had annual revenues of $50 million or more. Figure C1 shows the number of years of CISO in healthcare only.

Figure C10

Survey Round 1, Question 1 Analysis



Please indicate the number of years you have spent as a CISO (or equivalent) in a large U.S.-based healthcare organization with over $50M in annual revenue:

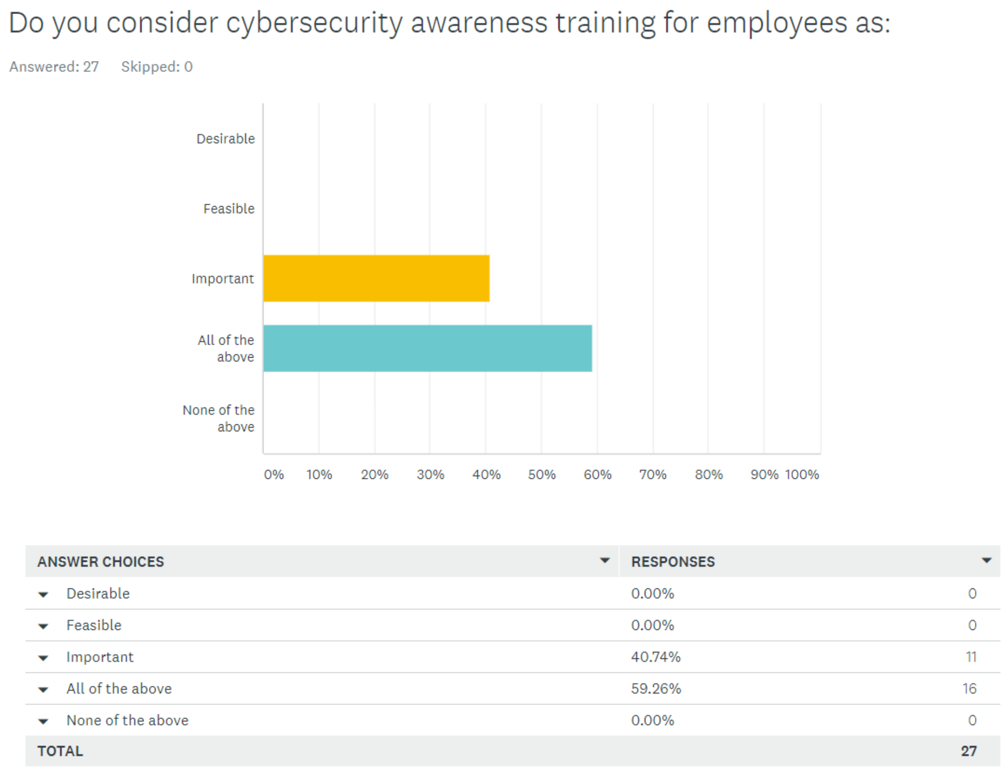
Answered: 27 Skipped: 0

ANSWER CHOICES	RESPONSES	
None	0.00%	0
1 - 3 years	11.11%	3
3 - 5 years	14.81%	4
5 - 10 years	51.85%	14
10+ years	22.22%	6
TOTAL		27

R1 Q2. This question asked if cybersecurity awareness training for employees was desirable, feasible, important, all the above, or none of the above. The results indicated 11 participants thought the training is important (not necessarily desirable or feasible), and 16 participants felt training was desirable, feasible, and important. This strategy will move forward with Round 2 survey questions.

Figure 11

Survey Round 1, Question 2 Analysis



Do you consider cybersecurity awareness training for employees as:

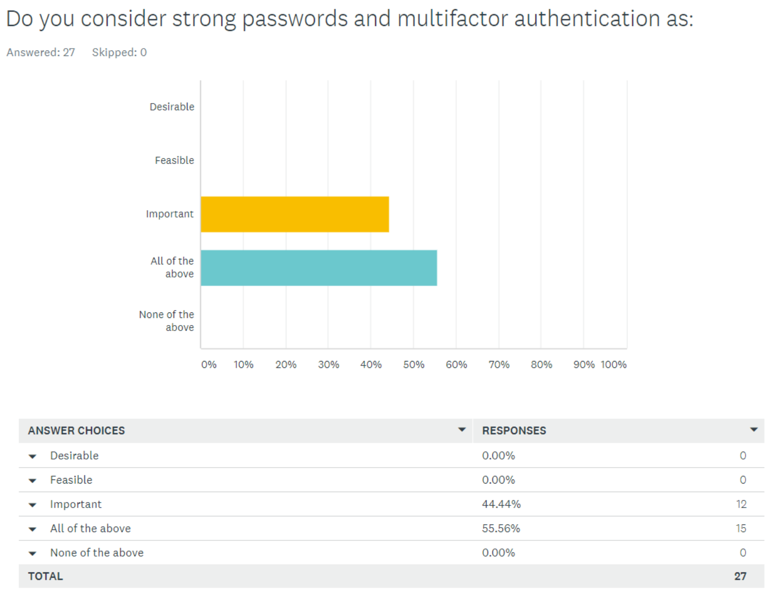
Answered: 27 Skipped: 0

ANSWER CHOICES	RESPONSES	
Desirable	0.00%	0
Feasible	0.00%	0
Important	40.74%	11
All of the above	59.26%	16
None of the above	0.00%	0
TOTAL		27

R1 Q3. Strong passwords include a requirement on the length of the password, usage of upper-case and lower-case alpha characters, numbers, special characters, etc., and multifactor authentication requires additional levels beyond just a user id and password to ensure the person requesting access is really that person. It could include sending a numeric code to the known email or phone number and having the individual enter the code as the second factor for authentication. Biometrics (e.g., retina scans, fingerprints, etc.) are also forms of multifactor authentication. The results showed that 12 participants felt these are important, but not desirable or feasible and 15 participants felt they were all three: desirable, feasible, and important. This strategy will move forward with Round 2 survey questions.

Figure 12

Survey Round 1, Question 3 Analysis



Do you consider strong passwords and multifactor authentication as:

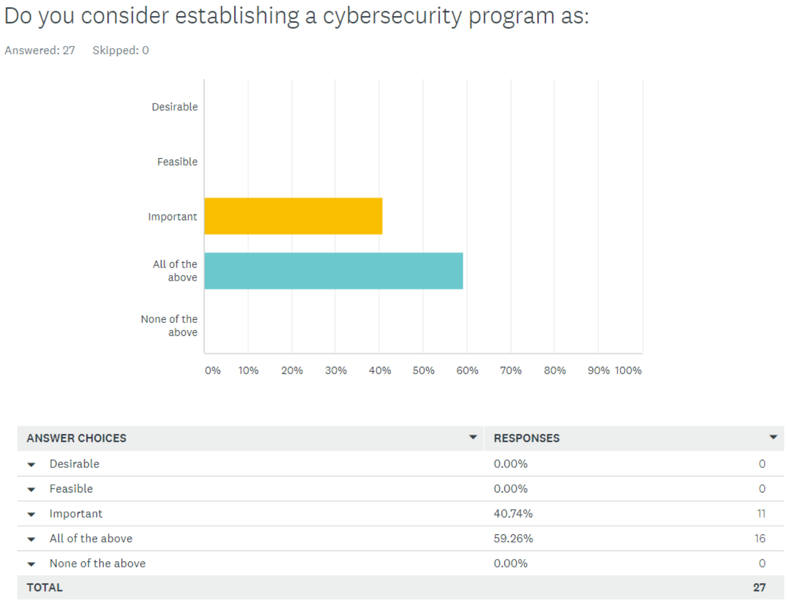
Answered: 27 Skipped: 0

ANSWER CHOICES	RESPONSES	
Desirable	0.00%	0
Feasible	0.00%	0
Important	44.44%	12
All of the above	55.56%	15
None of the above	0.00%	0
TOTAL		27

R1 Q4. Establishing a cybersecurity program was indicated as important to 11 participants and desirable, feasible, and important to 16 participants. Details of a cybersecurity program could include determining ultimate responsibility of cybersecurity, defining and documenting the roles and responsibilities of various teams, documenting and regularly reviewing policies and procedures and/or keeping evidence of the procedures to show they have been implemented. This strategy will move forward with Round 2 survey questions.

Figure 13

Survey Round 1, Question 4 Analysis



Do you consider establishing a cybersecurity program as:

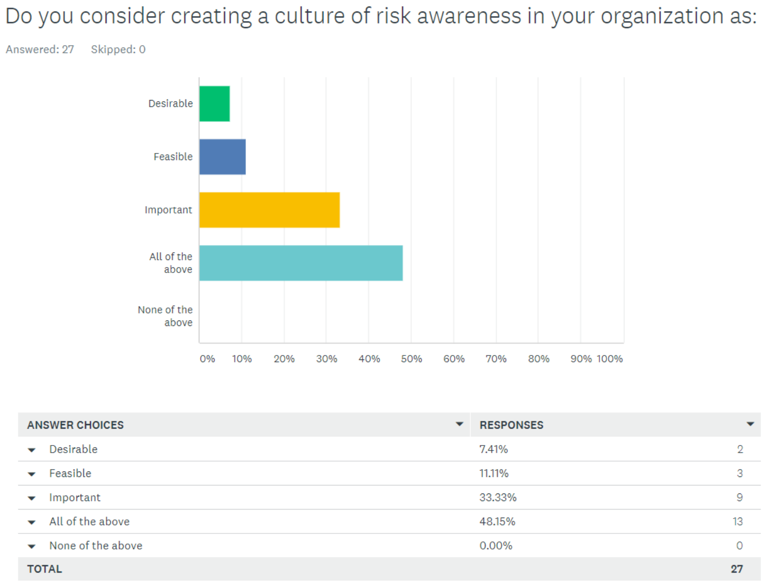
Answered: 27 Skipped: 0

ANSWER CHOICES	RESPONSES	
Desirable	0.00%	0
Feasible	0.00%	0
Important	40.74%	11
All of the above	59.26%	16
None of the above	0.00%	0
TOTAL		27

R1 Q5. The focus of this question was on developing the culture of risk awareness in an organization; it had some interesting results. Two participants considered this only as desirable, three participants indicated it as feasible, nine participants thought it was important, and 13 participants indicated all three: desirable, feasible, and important. The culture of an organization is a complex thing and may be difficult for some to grasp—a definition may have made this question clearer; however, CISOs should have a good understanding of culture. This item will not go forward onto Round 2 surveys as there were only 13 participants who indicated all three: desirable, feasible, and important.

Figure 14

Survey Round 1, Question 5 Analysis



Do you consider creating a culture of risk awareness in your organization as:

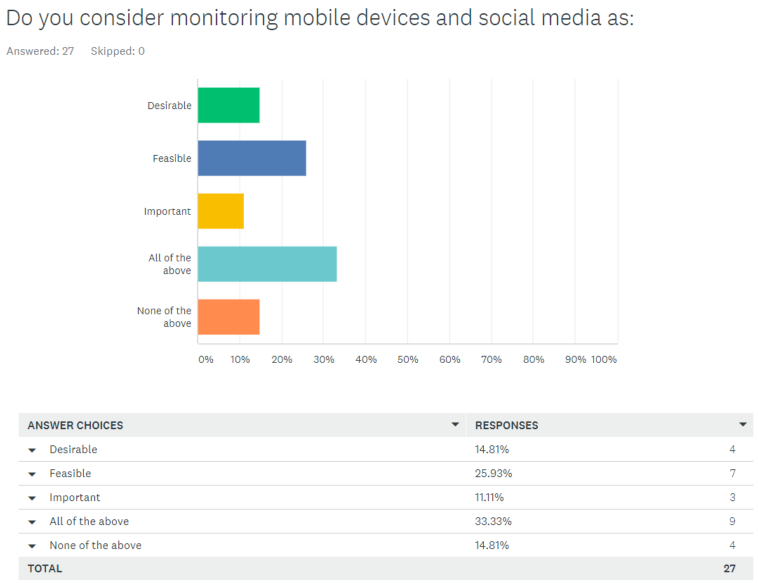
Answered: 27 Skipped: 0

ANSWER CHOICES	RESPONSES	
Desirable	7.41%	2
Feasible	11.11%	3
Important	33.33%	9
All of the above	48.15%	13
None of the above	0.00%	0
TOTAL		27

R1 Q6. Monitoring mobile devices and social media was the first question where there were *None of the Above* answers indicated. Four participants felt this was not desirable, feasible, or important. Four participants felt it was only desirable, seven participants felt it was only feasible, and three participants felt it was only important. Nine participants indicated all three: desirable, feasible, and important. Based on the responses provided, this strategy will not go forward into Round 2.

Figure 15

Survey Round 1, Question 6 Analysis



Do you consider monitoring mobile devices and social media as:

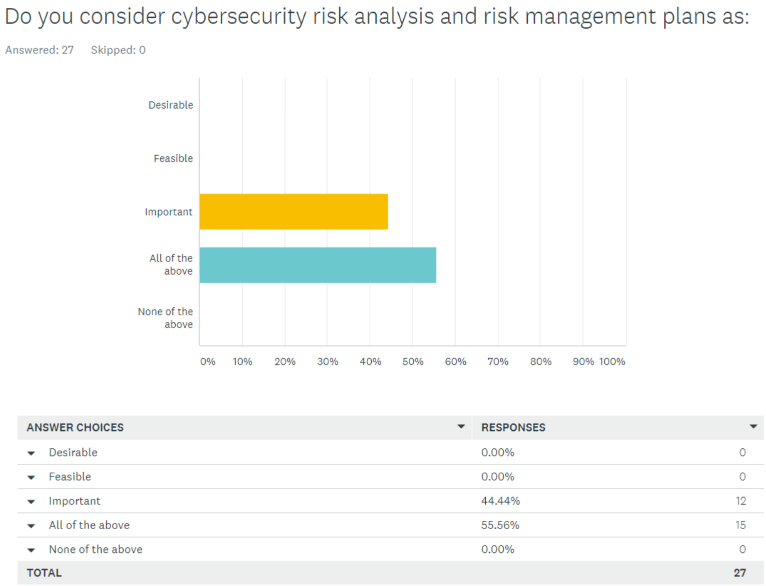
Answered: 27 Skipped: 0

ANSWER CHOICES	RESPONSES	
Desirable	14.81%	4
Feasible	25.93%	7
Important	11.11%	3
All of the above	33.33%	9
None of the above	14.81%	4
TOTAL		27

R1 Q7. Cybersecurity risk analysis and risk management plans were the focus of this question and 12 participants indicated it was important and 15 participants indicated it was all three: desirable, feasible, and important. As these items are required under the HIPAA Security Rule provisions for the security management processes, it was a positive indication that all the responses show that these should be done. This strategy will move forward with Round 2 survey questions.

Figure 16

Survey Round 1, Question 7 Analysis



Do you consider cybersecurity risk analysis and risk management plans as:

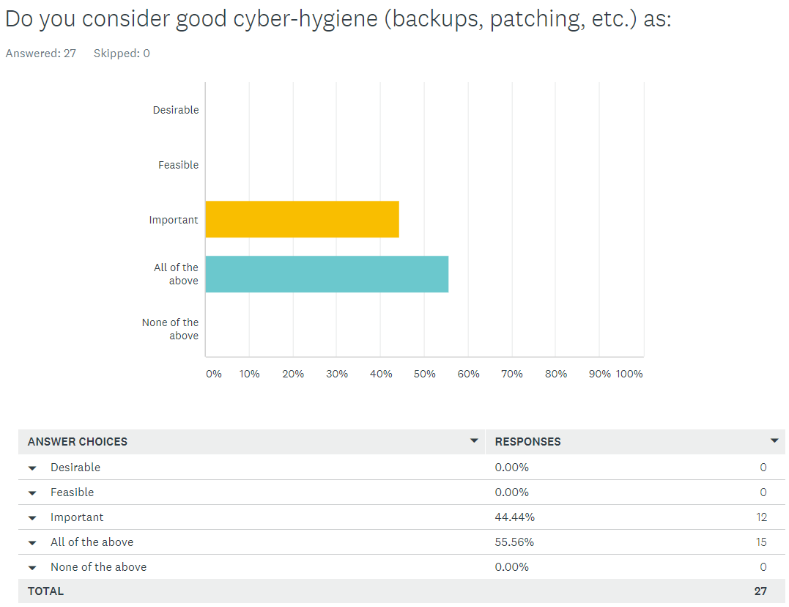
Answered: 27 Skipped: 0

ANSWER CHOICES	RESPONSES	
Desirable	0.00%	0
Feasible	0.00%	0
Important	44.44%	12
All of the above	55.56%	15
None of the above	0.00%	0
TOTAL		27

R1 Q8. Cyberhygiene includes keeping backups of systems and being able to recover them, and ensuring patches are installed in a timely manner. The responses to this question indicated 12 participants felt these are important; 15 participants indicated all three: desirable, feasible, and important. This strategy will move forward with Round 2 survey questions.

Figure 17

Survey Round 1, Question 8 Analysis



Do you consider good cyber-hygiene (backups, patching, etc.) as:

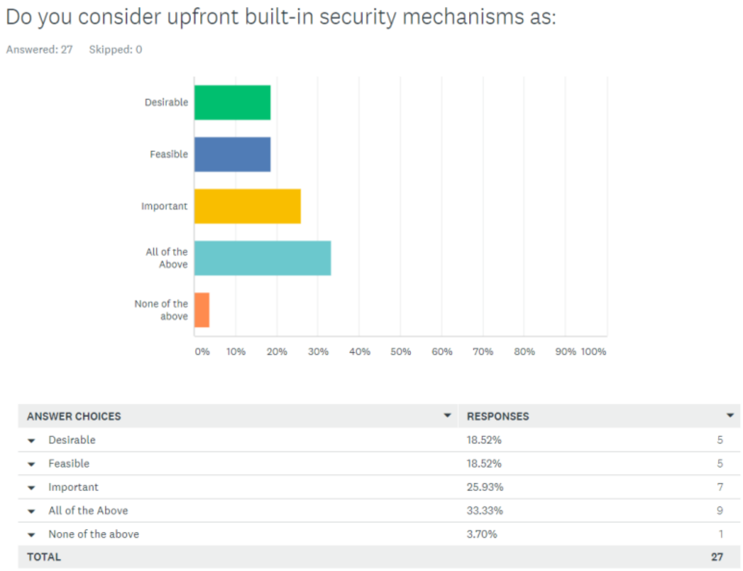
Answered: 27 Skipped: 0

ANSWER CHOICES	RESPONSES	
Desirable	0.00%	0
Feasible	0.00%	0
Important	44.44%	12
All of the above	55.56%	15
None of the above	0.00%	0
TOTAL		27

R1 Q9. Based on the responses, five participants indicated built-in security mechanisms as only desirable, five participants indicated it as only feasible, seven participants indicated it as important, and nine participants indicated it as all three: desirable, feasible, and important. One response indicated *None of the Above*. This strategy will not move forward with Round 2 survey questions.

Figure 18

Survey Round 1, Question 9 Analysis



Do you consider upfront built-in security mechanisms as:

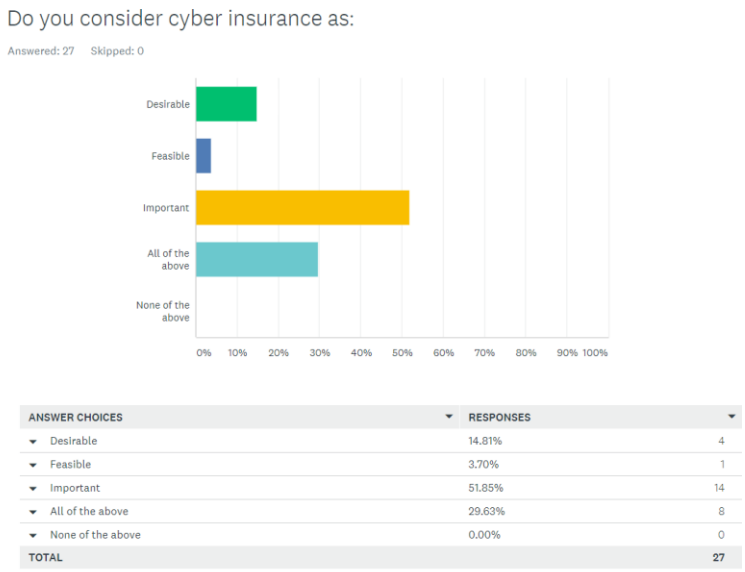
Answered: 27 Skipped: 0

ANSWER CHOICES	RESPONSES	
Desirable	18.52%	5
Feasible	18.52%	5
Important	25.93%	7
All of the Above	33.33%	9
None of the above	3.70%	1
TOTAL		27

R1 Q10. Cyber insurance was deemed as desirable by four participants, feasible by one participant, important to 14 participants, and only eight participants indicated it as all three: desirable, feasible, and important. This strategy will not go forward into Round 2 survey questions.

Figure 19

Survey Round 1, Question 10 Analysis



Do you consider cyber insurance as:

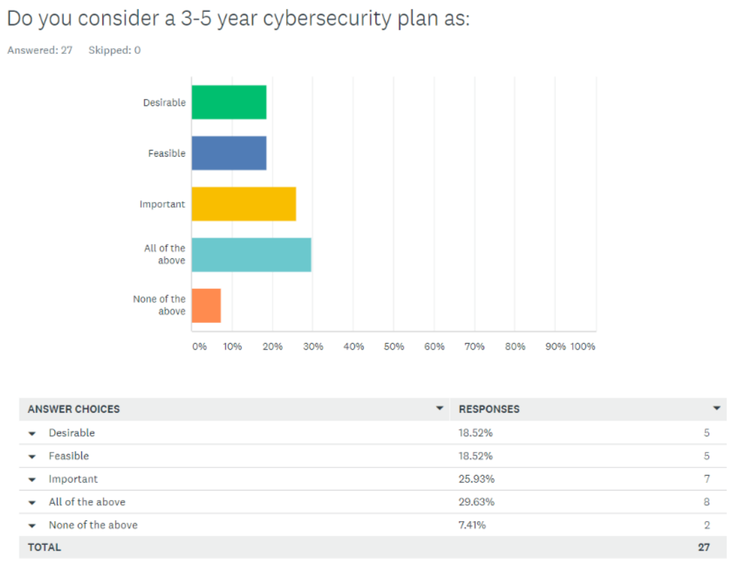
Answered: 27 Skipped: 0

ANSWER CHOICES	RESPONSES	
Desirable	14.81%	4
Feasible	3.70%	1
Important	51.85%	14
All of the above	29.63%	8
None of the above	0.00%	0
TOTAL		27

R1 Q11. A 3-to-5-year cybersecurity plan was desirable to five participants, feasible to five participants, important to seven participants, eight participants showed all three: desirable, feasible, and important; and two participants selected *None of the Above*. When comparing to RQ7 on risk analysis and risk management plans, the answers are surprisingly different. It was expected that the risk management plan in RQ7 would show what strategies will be implemented over the next 3–5 years. This strategy will not go forward into Round 2 survey questions.

Figure 20

Survey Round 1, Question 11 Analysis



Do you consider a 3-5 year cybersecurity plan as:

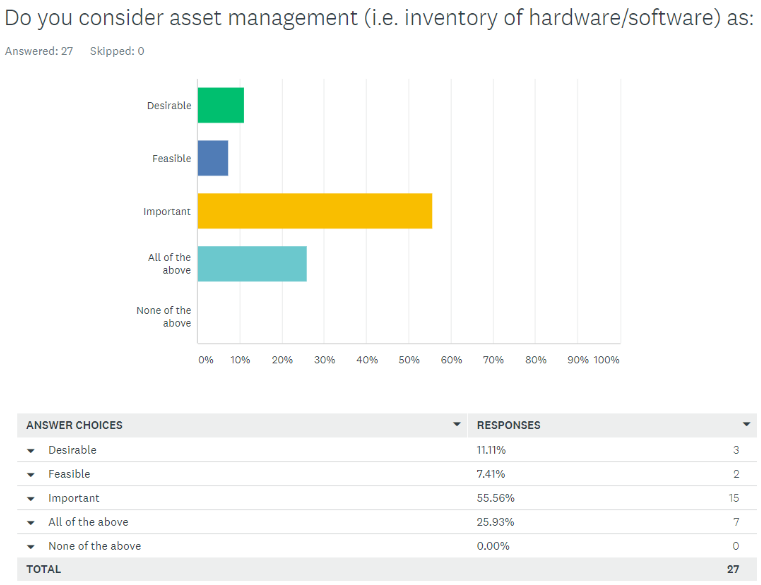
Answered: 27 Skipped: 0

ANSWER CHOICES	RESPONSES	
Desirable	18.52%	5
Feasible	18.52%	5
Important	25.93%	7
All of the above	29.63%	8
None of the above	7.41%	2
TOTAL		27

R1 Q12. Answers for this question were also surprising. If an organization does not have an inventory of all hardware and software, it cannot manage what it does not know about. An example is an older server that requires patching is not included on the list of servers to be patched. It is unknown and exposes the organization to a vulnerability they are not even aware of. Attackers take advantage of organizations not managing their equipment. Three participants indicated it as desirable, two participants indicated it as feasible, fifteen participants indicated it as important, and only seven participants indicated it as all three: desirable, feasible, and important. This strategy will not go forward into Round 2 due to the low number of all three.

Figure 21

Survey Round 1, Question 12 Analysis



Do you consider asset management (i.e. inventory of hardware/software) as:

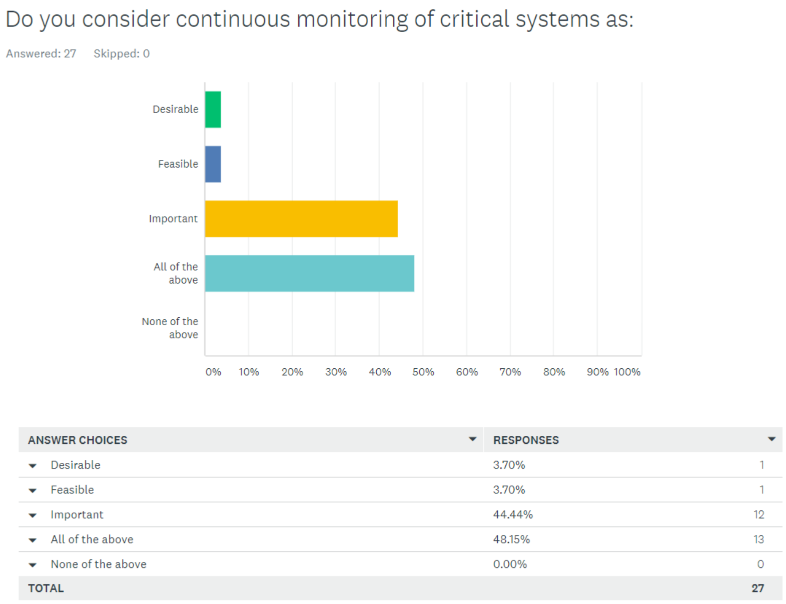
Answered: 27 Skipped: 0

ANSWER CHOICES	RESPONSES	
Desirable	11.11%	3
Feasible	7.41%	2
Important	55.56%	15
All of the above	25.93%	7
None of the above	0.00%	0
TOTAL		27

R1 Q13. Continuous monitoring of critical systems includes 24x7 monitoring for nefarious activities and, if an attack is detected, will send alerts to specific support individuals who will take appropriate incident response actions. One participant indicated this is desirable, one participant indicated this is feasible, twelve participants thought it is important, and thirteen participants indicated all three: desirable, feasible, and important. There were also some comments on this topic in the free text question at the end, which is overlapping this question. This strategy will move forward with Round 2 survey questions.

Figure 22

Survey Round 1, Question 13 Analysis



Do you consider continuous monitoring of critical systems as:

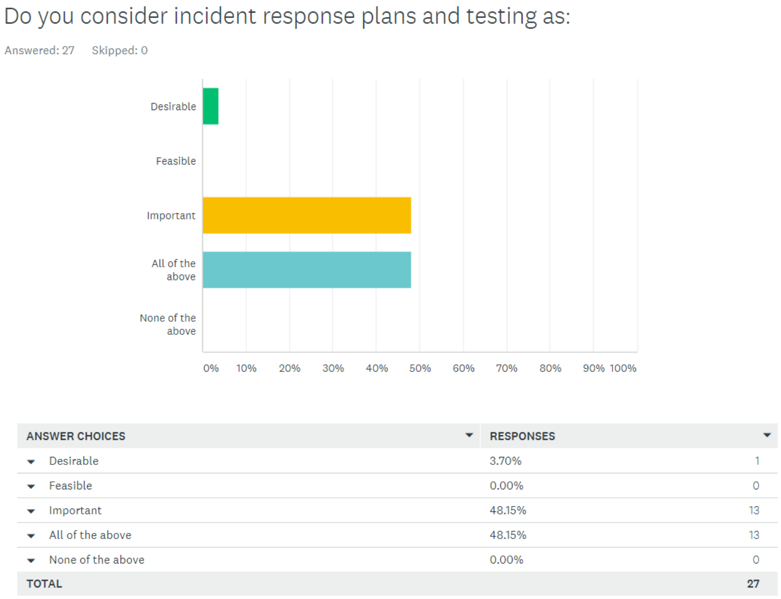
Answered: 27 Skipped: 0

ANSWER CHOICES	RESPONSES	
Desirable	3.70%	1
Feasible	3.70%	1
Important	44.44%	12
All of the above	48.15%	13
None of the above	0.00%	0
TOTAL		27

R1 Q14. Incident response plans and testing include documented steps of what actions should be taken in various situations. Testing of the plans should be done on a regular basis to ensure teams understand what actions need to be taken. One example of this would be during a ransomware attack, a copy of the infected system should be made prior to restoring from backup. The restoration would erase all forensic evidence to show what happened. One participant indicated this is desirable, thirteen participants indicated it was important, and thirteen participants indicated it was all three: desirable, feasible, and important. This strategy will move forward with Round 2 survey questions.

Figure 23

Survey Round 1, Question 14 Analysis



Do you consider incident response plans and testing as:

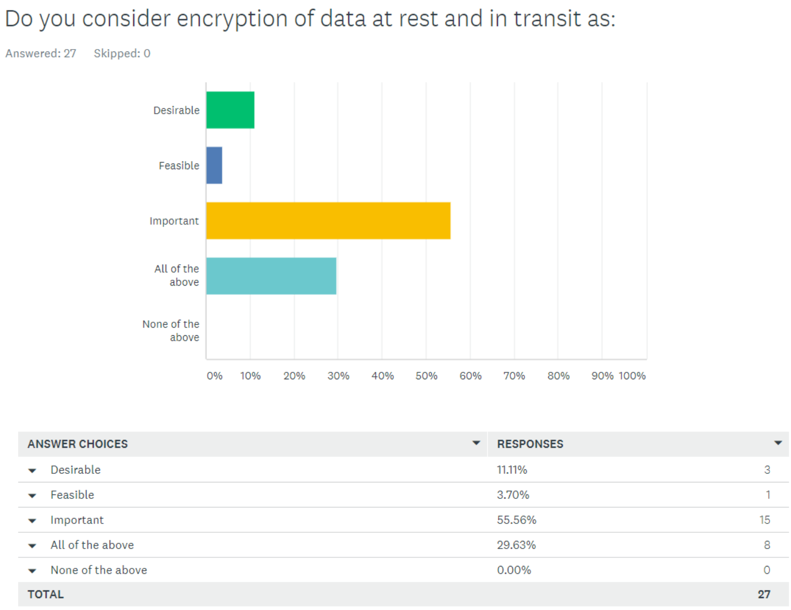
Answered: 27 Skipped: 0

ANSWER CHOICES	RESPONSES	
Desirable	3.70%	1
Feasible	0.00%	0
Important	48.15%	13
All of the above	48.15%	13
None of the above	0.00%	0
TOTAL		27

R1 Q15. Encryption of data at rest and in transit is a controversial topic in many organizations. The results on this strategy shows three participants indicated it is desirable, one participant indicated it is feasible, 15 participants indicated it is important, and only eight participants indicated it is all three: desirable, feasible, and important. Due to the low number of participants indicated all three, this strategy will be dropped from going forward in the second round of surveys.

Figure 24

Survey Round 1, Question 15 Analysis



Do you consider encryption of data at rest and in transit as:

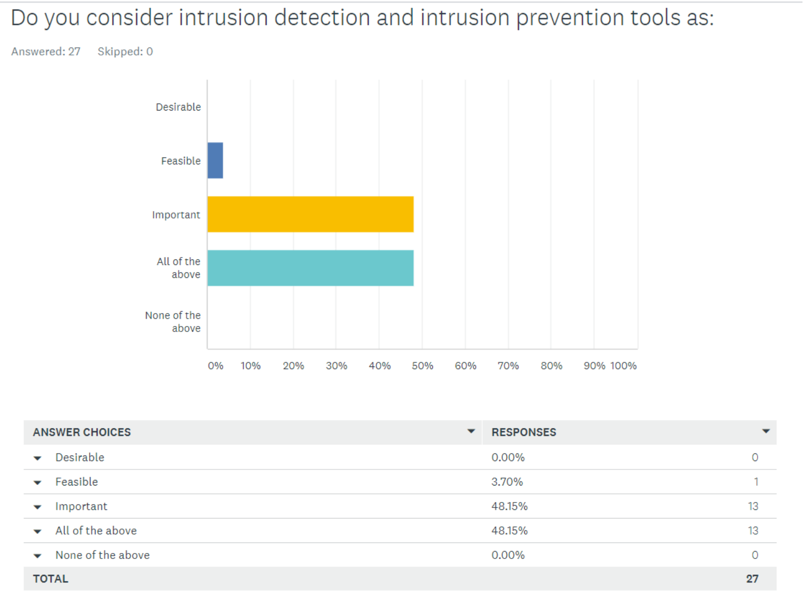
Answered: 27   Skipped: 0

ANSWER CHOICES	RESPONSES	
Desirable	11.11%	3
Feasible	3.70%	1
Important	55.56%	15
All of the above	29.63%	8
None of the above	0.00%	0
TOTAL		27

R1 Q16. When an attack is detected, intrusion detection and intrusion protection tools are automated mechanisms that will alert proper staff to stop the attack, hopefully before much damage is done. Tools put in place that are protecting the environment is more proactive and, generally, a better way to keep systems secure. The results for this strategy show only one participant thinks it is only feasible, while thirteen participants indicated it was important, and thirteen participants indicated all three: desirable, feasible, and important. This strategy will continue into Round 2 survey questions.

Figure 25

Survey Round 1, Question 16 Analysis



Do you consider intrusion detection and intrusion prevention tools as:

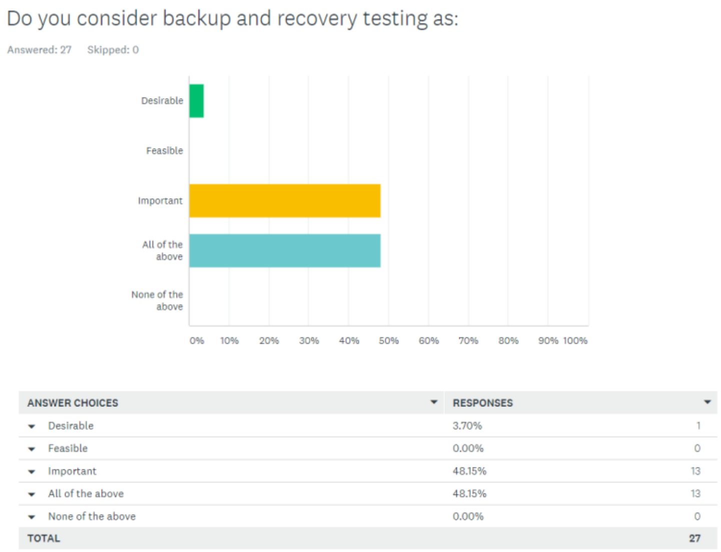
Answered: 27 Skipped: 0

ANSWER CHOICES	RESPONSES	
Desirable	0.00%	0
Feasible	3.70%	1
Important	48.15%	13
All of the above	48.15%	13
None of the above	0.00%	0
TOTAL		27

R1 Q17. Backup and recovery testing is an important defense and used as a strategy when ransomware attacks are made. When the hacker encrypts your system and demands ransom, the backup can be recovered and the ransom would not need to be paid. However, some backups are also encrypted by the attacker with the ransomware, leaving the organization with no options but to pay. The results for this question show one participant indicated it is only desirable, while thirteen participants indicated it as important, and thirteen participants indicated all three: desirable, feasible, and important. This item will move onto the next round of surveys.

Figure 26

Survey Round 1, Question 17 Analysis



Do you consider backup and recovery testing as:

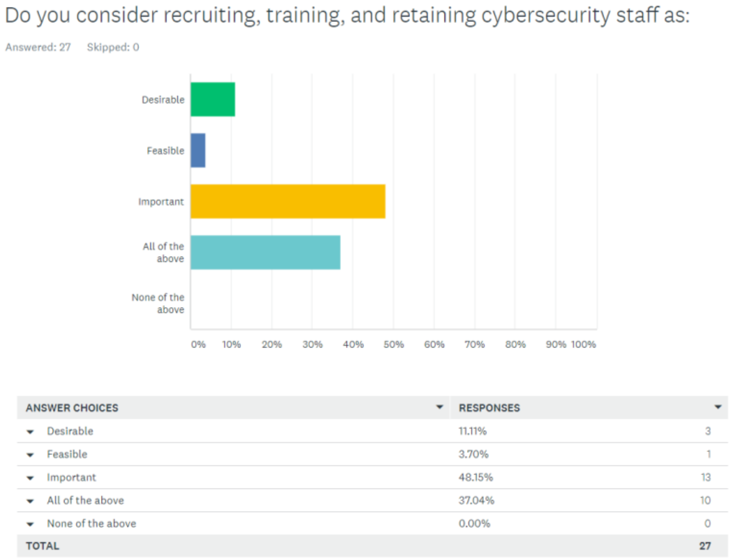
Answered: 27 Skipped: 0

ANSWER CHOICES	RESPONSES	
Desirable	3.70%	1
Feasible	0.00%	0
Important	48.15%	13
All of the above	48.15%	13
None of the above	0.00%	0
TOTAL		27

R1 Q18. Recruiting, training, and retaining cybersecurity staff was not a strategy that participants felt strongly about. Three participants felt this strategy was desirable, one participant indicated feasible, thirteen participants thought it was important, and only 10 participants showed it as all three: desirable, feasible, and important. This item will not go forward onto Round 2 surveys.

Figure 27

Survey Round 1, Question 18 Analysis



Do you consider recruiting, training, and retaining cybersecurity staff as:

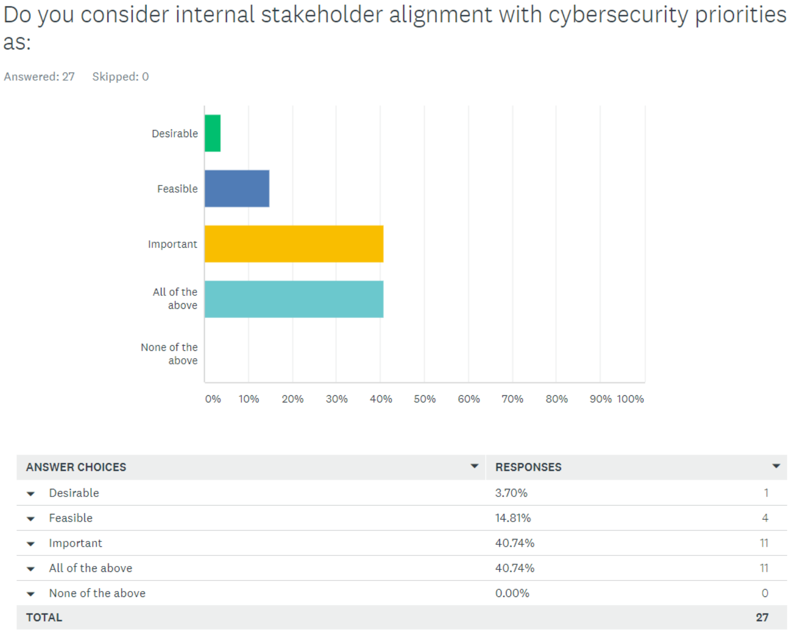
Answered: 27 Skipped: 0

ANSWER CHOICES	RESPONSES	
Desirable	11.11%	3
Feasible	3.70%	1
Important	48.15%	13
All of the above	37.04%	10
None of the above	0.00%	0
TOTAL		27

R1 Q19. Internal stakeholder alignment with cybersecurity priorities includes the different business areas in the organization and agrees with the cybersecurity priorities in the plan. If there is no alignment, the funding for activities is not made available, making it difficult to protect the organization. One participant indicated that this is desirable, four participants indicated this is feasible, eleven participants indicated this is important, and eleven participants indicated all three: desirable, feasible, and important. This strategy will not move forward with Round 2 survey questions.

Figure 28

Survey Round 1, Question 19 Analysis



Do you consider internal stakeholder alignment with cybersecurity priorities as:

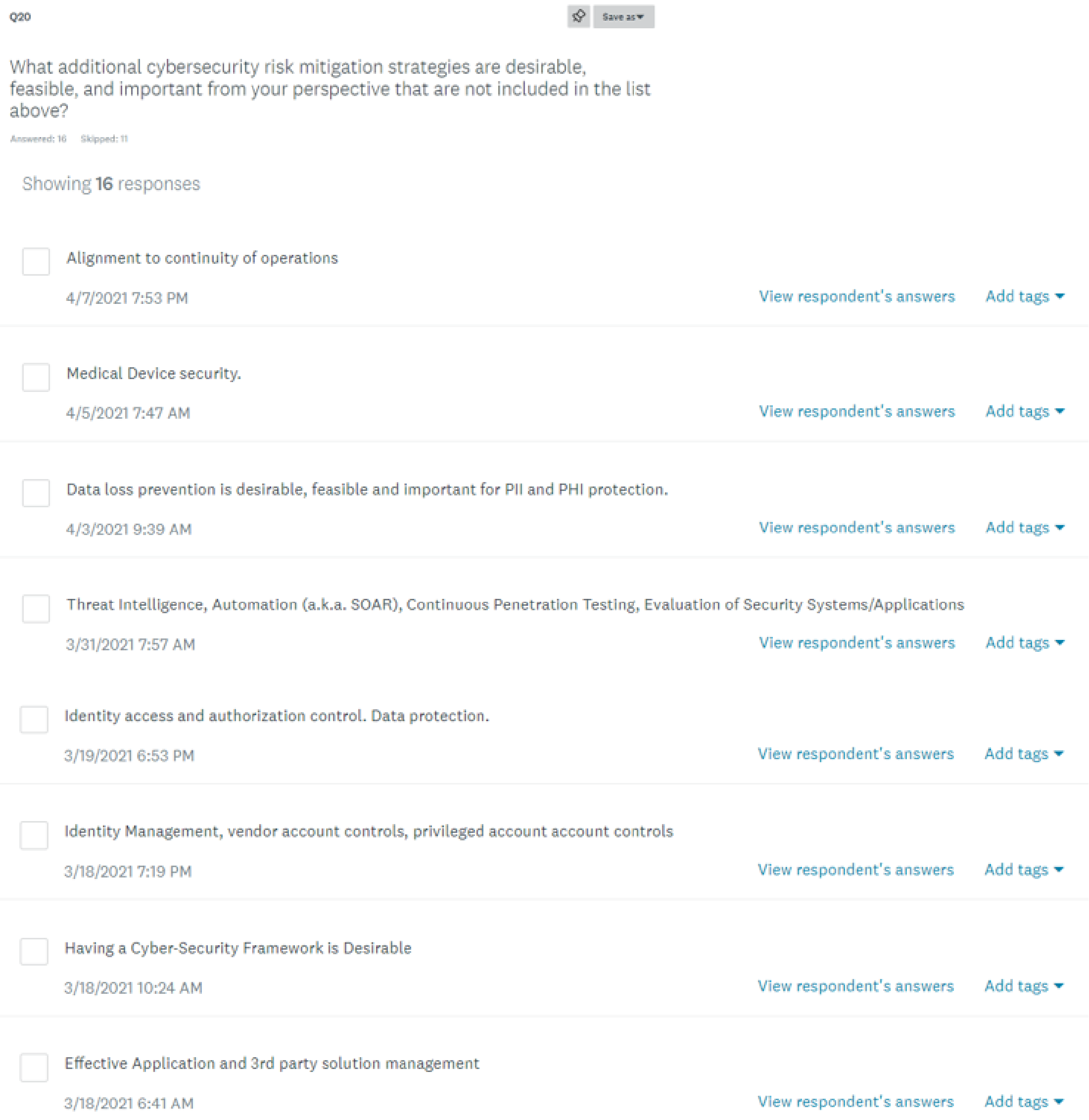
Answered: 27 Skipped: 0

ANSWER CHOICES	RESPONSES	
Desirable	3.70%	1
Feasible	14.81%	4
Important	40.74%	11
All of the above	40.74%	11
None of the above	0.00%	0
TOTAL		27

R1 Q20. The last Round 1 question allowed the participants to type in additional cybersecurity risk mitigation strategies in the free text area as shown in Figure 29.

Figure 29

Survey Round 1, Question 19 Analysis



Q20

What additional cybersecurity risk mitigation strategies are desirable, feasible, and important from your perspective that are not included in the list above?

Answered: 16 Skipped: 11

Showing **16** responses

□ Alignment to continuity of operations
4/7/2021 7:53 PM

□ Medical Device security.
4/5/2021 7:47 AM

□ Data loss prevention is desirable, feasible and important for PII and PHI protection.
4/3/2021 9:39 AM

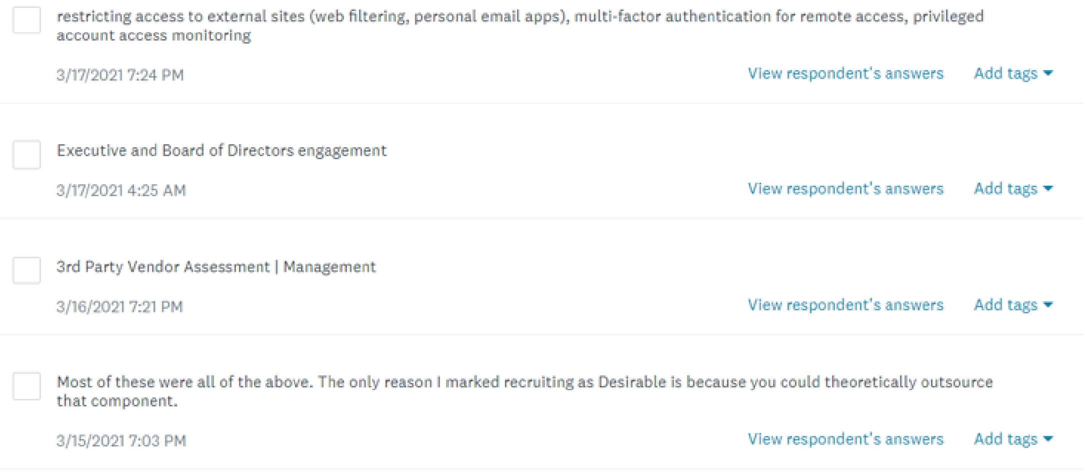
□ Threat Intelligence, Automation (a.k.a. SOAR), Continuous Penetration Testing, Evaluation of Security Systems/Applications
3/31/2021 7:57 AM

□ Identity access and authorization control. Data protection.
3/19/2021 6:53 PM

□ Identity Management, vendor account controls, privileged account account controls
3/18/2021 7:19 PM

□ Having a Cyber-Security Framework is Desirable
3/18/2021 10:24 AM

□ Effective Application and 3rd party solution management
3/18/2021 6:41 AM



☐ restricting access to external sites (web filtering, personal email apps), multi-factor authentication for remote access, privileged account access monitoring

3/17/2021 7:24 PM

View respondent's answers
Add tags ▾

☐ Executive and Board of Directors engagement

3/17/2021 4:25 AM

View respondent's answers
Add tags ▾

☐ 3rd Party Vendor Assessment | Management

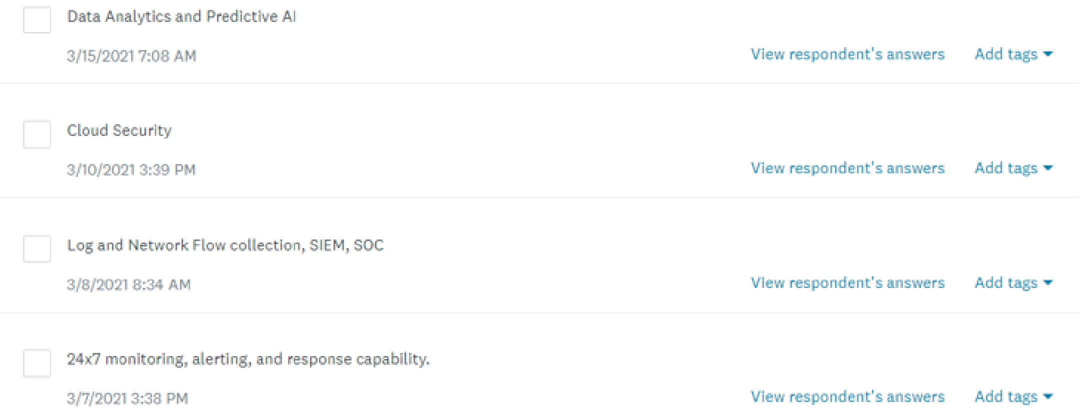
3/16/2021 7:21 PM

View respondent's answers
Add tags ▾

☐ Most of these were all of the above. The only reason I marked recruiting as Desirable is because you could theoretically outsource that component.

3/15/2021 7:03 PM

View respondent's answers
Add tags ▾



☐ Data Analytics and Predictive AI

3/15/2021 7:08 AM

View respondent's answers
Add tags ▾

☐ Cloud Security

3/10/2021 3:39 PM

View respondent's answers
Add tags ▾

☐ Log and Network Flow collection, SIEM, SOC

3/8/2021 8:34 AM

View respondent's answers
Add tags ▾

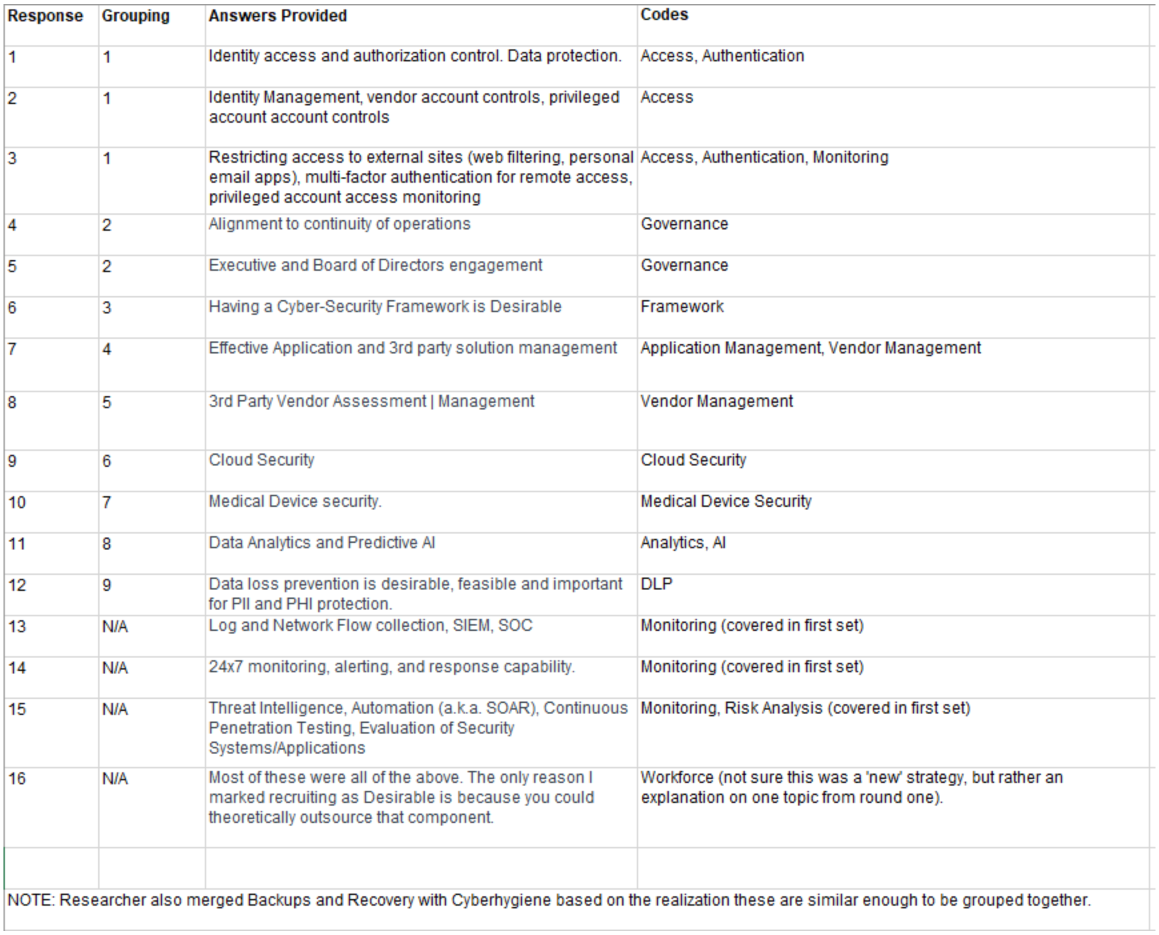
☐ 24x7 monitoring, alerting, and response capability.

3/7/2021 3:38 PM

View respondent's answers
Add tags ▾

Figure 30

Survey Round 1, Question 20 Analysis and Coding—New Strategies



Response	Grouping	Answers Provided	Codes
1	1	Identity access and authorization control. Data protection.	Access, Authentication
2	1	Identity Management, vendor account controls, privileged account account controls	Access
3	1	Restricting access to external sites (web filtering, personal email apps), multi-factor authentication for remote access, privileged account access monitoring	Access, Authentication, Monitoring
4	2	Alignment to continuity of operations	Governance
5	2	Executive and Board of Directors engagement	Governance
6	3	Having a Cyber-Security Framework is Desirable	Framework
7	4	Effective Application and 3rd party solution management	Application Management, Vendor Management
8	5	3rd Party Vendor Assessment | Management	Vendor Management
9	6	Cloud Security	Cloud Security
10	7	Medical Device security.	Medical Device Security
11	8	Data Analytics and Predictive AI	Analytics, AI
12	9	Data loss prevention is desirable, feasible and important for PII and PHI protection.	DLP
13	N/A	Log and Network Flow collection, SIEM, SOC	Monitoring (covered in first set)
14	N/A	24x7 monitoring, alerting, and response capability.	Monitoring (covered in first set)
15	N/A	Threat Intelligence, Automation (a.k.a. SOAR), Continuous Penetration Testing, Evaluation of Security Systems/Applications	Monitoring, Risk Analysis (covered in first set)
16	N/A	Most of these were all of the above. The only reason I marked recruiting as Desirable is because you could theoretically outsource that component.	Workforce (not sure this was a 'new' strategy, but rather an explanation on one topic from round one).

NOTE: Researcher also merged Backups and Recovery with Cyberhygiene based on the realization these are similar enough to be grouped together.

Appendix D: Round 2 Survey Questions

The following information was sent to all participants to let them know that Round 2 of the survey is coming:

> "Thank you for your responses from Round 1 of the survey for the Delphi study. The information was utilized to create Round 2 of the survey. The link for Round 2 of the survey will be emailed via SurveyMonkey within the next few days. Please respond within 48 hours of receipt of the email. Thank you again!"

Instructions for Q1:

Included below are the top eight risk remediation categories based on desirability, feasibility, and importance from the results of the first round of the survey. Please rank from 1 (highest) to 8 (lowest) in order of desirability, feasibility, and importance by dropping and dragging into the correct prioritized order:

- Cybersecurity Awareness and Training
- Strong Passwords and Multifactor Authentication
- Establishing a Cybersecurity Program
- Risk Analysis and Risk Management Plan
- Cybersecurity Hygiene (backups, patching, recovery testing, etc.)
- Continuous Monitoring of Critical Systems
- Incident Response Plans and Testing
- Intrusion Detection and Prevention Tools

Instructions for Q2 through Q11:

In the first round of the survey, the last question, Q20, was:

> "What additional cybersecurity risk mitigation strategies are desirable, feasible, and important, from your perspective, that are not included in the list above?"

Your responses were analyzed and, if the response was not related to one of the Round 1 categories, they were grouped into logically related categories. The following eleven additional categories are included in Q2 through Q11 of Round 2 below.

Please indicate your opinion by checking applicable boxes for each category as to whether you consider them to be desirable, feasible, important, or none of the above. Rather than multiple-choice selections with only one answer, these are selection boxes where you can choose multiple answers.

Note: As with the first round of the survey, for the next 11 questions, *desirable*, *feasible,* and *important* have the following meaning:

Desirable: something that is wanted.

Feasible: something that is possible.

Important: something that must be done.

Q2—Identity Access Management (all system accounts including vendor and privileged accounts are appropriately provisioned, deprovisioned, and regularly reviewed)

Desirable

Feasible

Important

None of the above

Q3—Governance (executive and board level engagement, alignment to operations)

Desirable

Feasible

Important

None of the above

Q4—Cybersecurity Frameworks (i.e., NIST, HIPAA, ISO)

Desirable

Feasible

Important

None of the above

Q5—Cybersecurity Policy and Procedures (documented, regularly reviewed and updated)

Desirable

Feasible

Important

None of the above

Q6—Third-Party Vendor Management (Assessing, Business Associate Agreements)

Desirable

Feasible

Important

None of the above

Q7—Application Management (Changes, Releases, Testing, etc.)

Desirable

Feasible

Important

None of the above

Q8—Cloud Security

Desirable

Feasible

Important

None of the above

Q9—Medical Device Security

Desirable

Feasible

Important

None of the above

Q10—Data Analytics and Predictive Artificial Intelligence (AI)

Desirable

Feasible

Important

None of the above

Q11—Data Loss Prevention (tools to stop exfiltration)

Desirable

Feasible

Important

None of the above

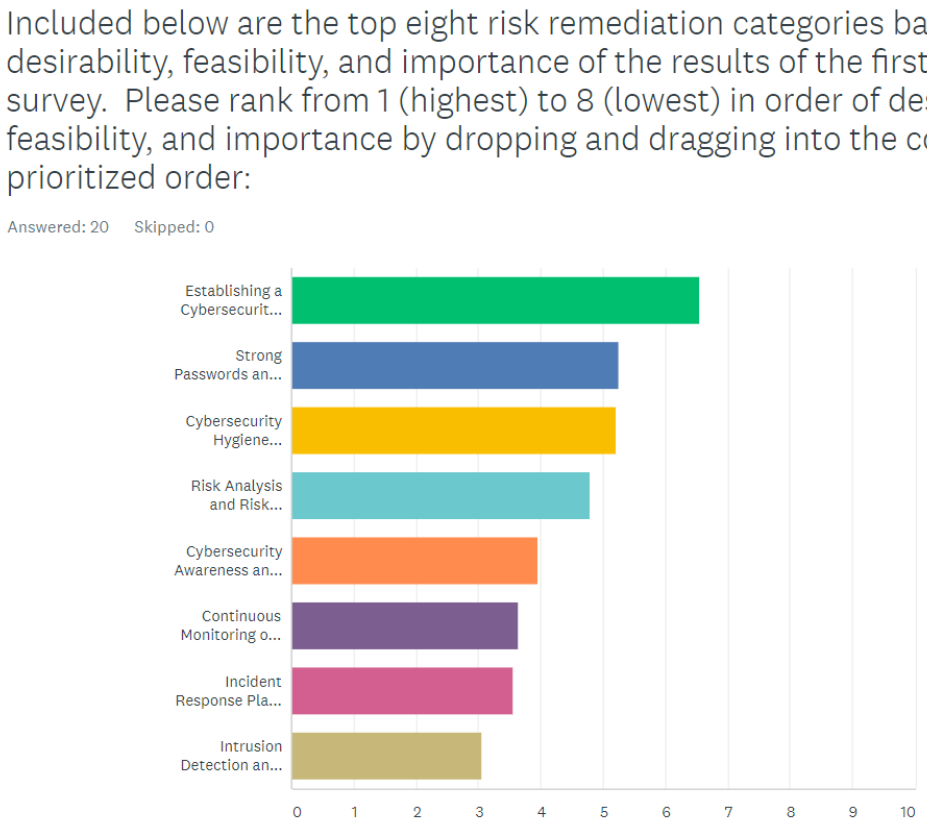
Q12—Please provide any feedback or questions you have for the researcher below:

Appendix E: Round 2 Survey Responses

R2 Q1:

Figure 31

Survey Round 2, Question 1 Results



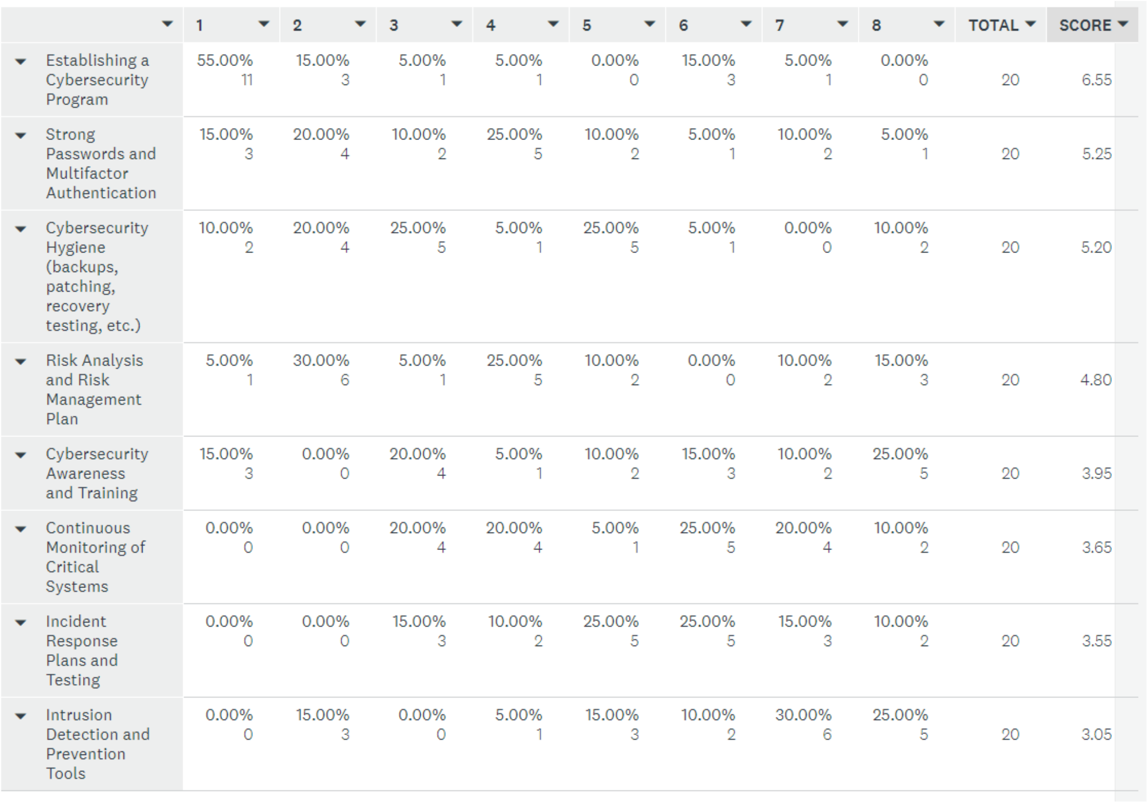
Included below are the top eight risk remediation categories based on the desirability, feasibility, and importance of the results of the first round of the survey. Please rank from 1 (highest) to 8 (lowest) in order of desirability, feasibility, and importance by dropping and dragging into the correct prioritized order:

Answered: 20 Skipped: 0

Establishing a Cybersecurit...
Strong Passwords an...
Cybersecurity Hygiene...
Risk Analysis and Risk...
Cybersecurity Awareness an...
Continuous Monitoring o...
Incident Response Pla...
Intrusion Detection an...
0
1
2
3
4
5
6
7
8
9
10

Figure 32

Survey Round 2, Question 1 Data



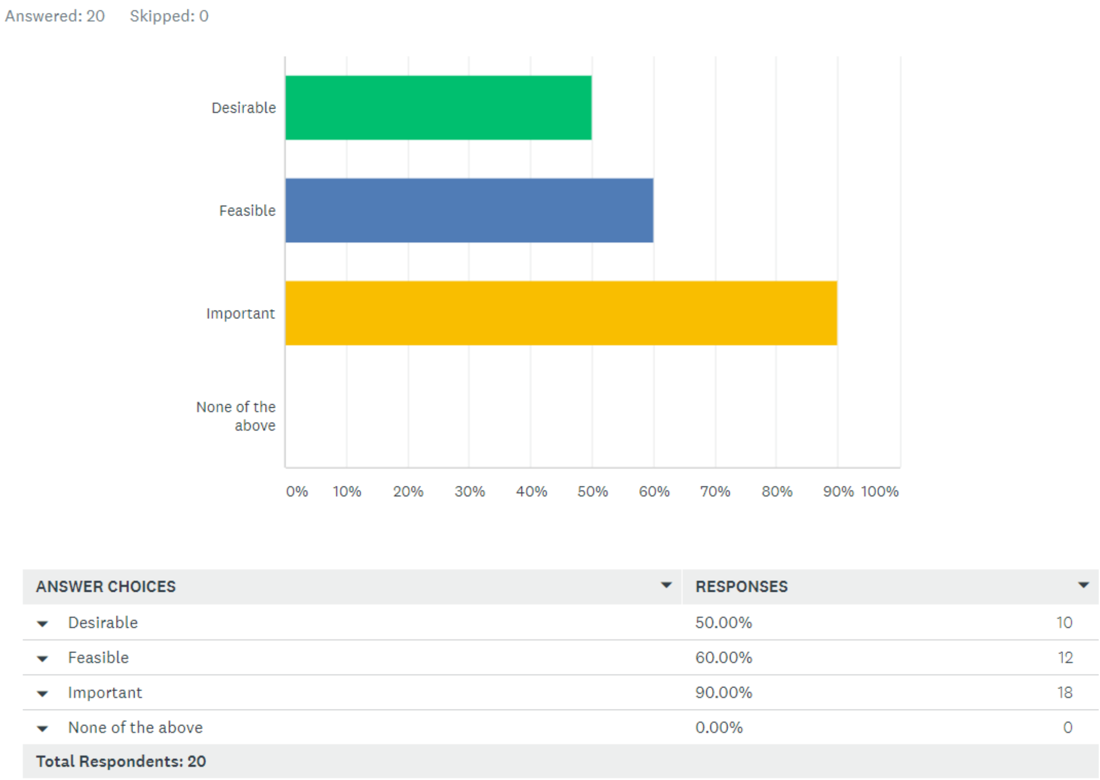
	1	2	3	4	5	6	7	8	TOTAL	SCORE
Establishing a Cybersecurity Program	55.00% 11	15.00% 3	5.00% 1	5.00% 1	0.00% 0	15.00% 3	5.00% 1	0.00% 0	20	6.55
Strong Passwords and Multifactor Authentication	15.00% 3	20.00% 4	10.00% 2	25.00% 5	10.00% 2	5.00% 1	10.00% 2	5.00% 1	20	5.25
Cybersecurity Hygiene (backups, patching, recovery testing, etc.)	10.00% 2	20.00% 4	25.00% 5	5.00% 1	25.00% 5	5.00% 1	0.00% 0	10.00% 2	20	5.20
Risk Analysis and Risk Management Plan	5.00% 1	30.00% 6	5.00% 1	25.00% 5	10.00% 2	0.00% 0	10.00% 2	15.00% 3	20	4.80
Cybersecurity Awareness and Training	15.00% 3	0.00% 0	20.00% 4	5.00% 1	10.00% 2	15.00% 3	10.00% 2	25.00% 5	20	3.95
Continuous Monitoring of Critical Systems	0.00% 0	0.00% 0	20.00% 4	20.00% 4	5.00% 1	25.00% 5	20.00% 4	10.00% 2	20	3.65
Incident Response Plans and Testing	0.00% 0	0.00% 0	15.00% 3	10.00% 2	25.00% 5	25.00% 5	15.00% 3	10.00% 2	20	3.55
Intrusion Detection and Prevention Tools	0.00% 0	15.00% 3	0.00% 0	5.00% 1	15.00% 3	10.00% 2	30.00% 6	25.00% 5	20	3.05

R2 Q2:

Identity Access Management (ensures all system accounts including vendor and privileged accounts are appropriately provisioned, deprovisioned, and regularly reviewed).

Figure 33

Survey Round 2, Question 2 Results



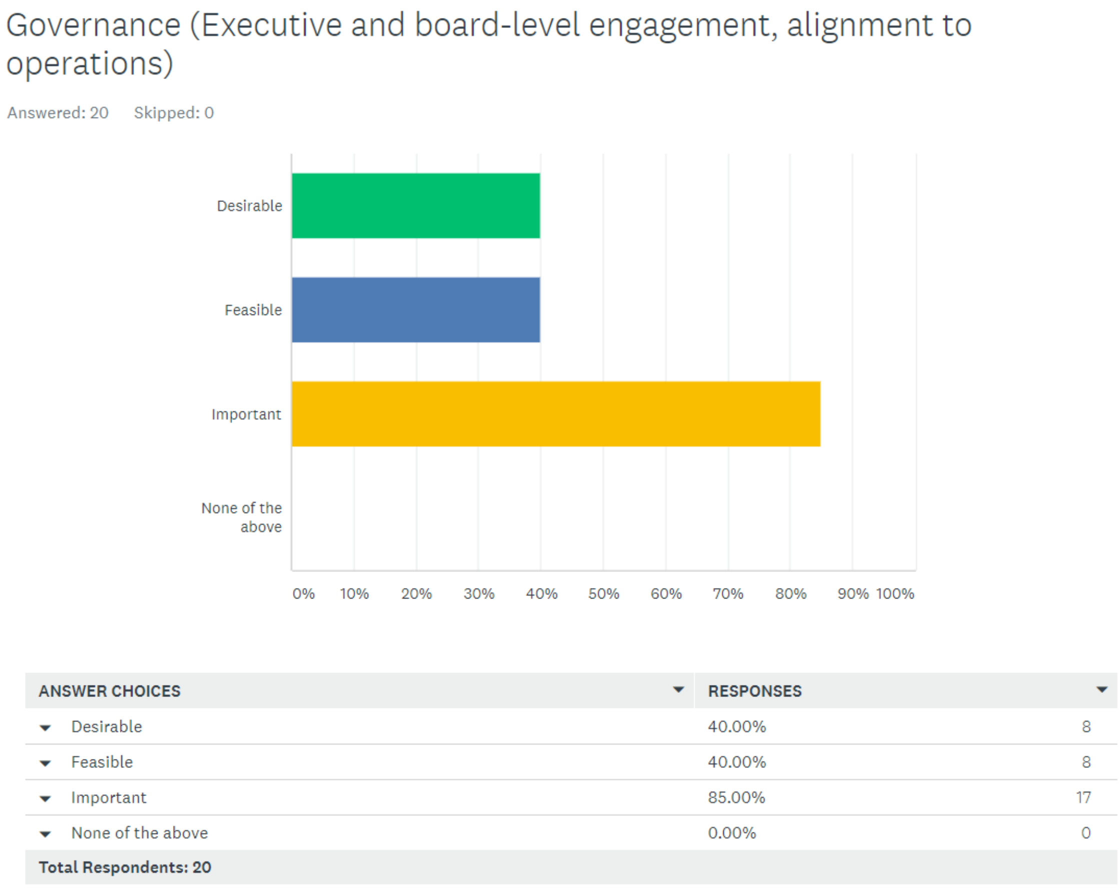
Answered: 20 Skipped: 0

ANSWER CHOICES	RESPONSES	
Desirable	50.00%	10
Feasible	60.00%	12
Important	90.00%	18
None of the above	0.00%	0
Total Respondents: 20		

R2 Q3:

Figure 34

Survey Round 2, Question 3 Results



Governance (Executive and board-level engagement, alignment to operations)

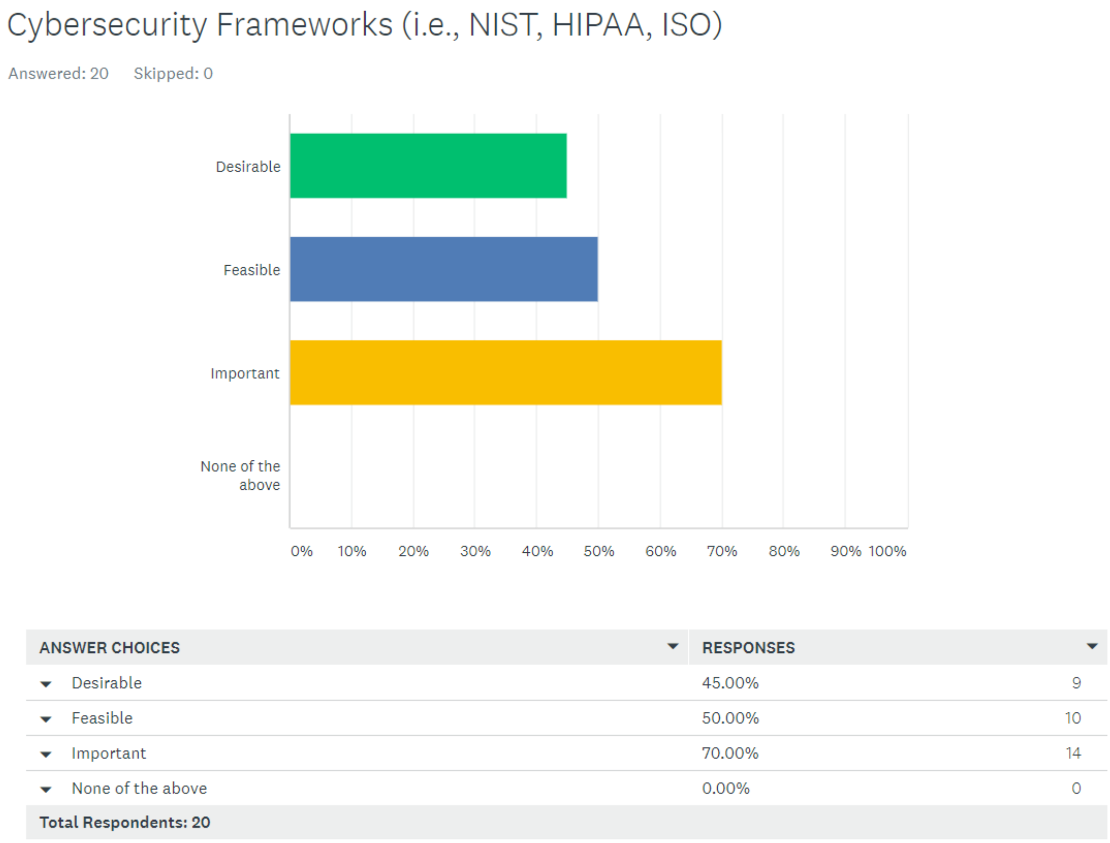
Answered: 20 Skipped: 0

ANSWER CHOICES	RESPONSES	
Desirable	40.00%	8
Feasible	40.00%	8
Important	85.00%	17
None of the above	0.00%	0
Total Respondents: 20		

R2 Q4:

Figure 35

Survey Round 2, Question 4 Results



Cybersecurity Frameworks (i.e., NIST, HIPAA, ISO)

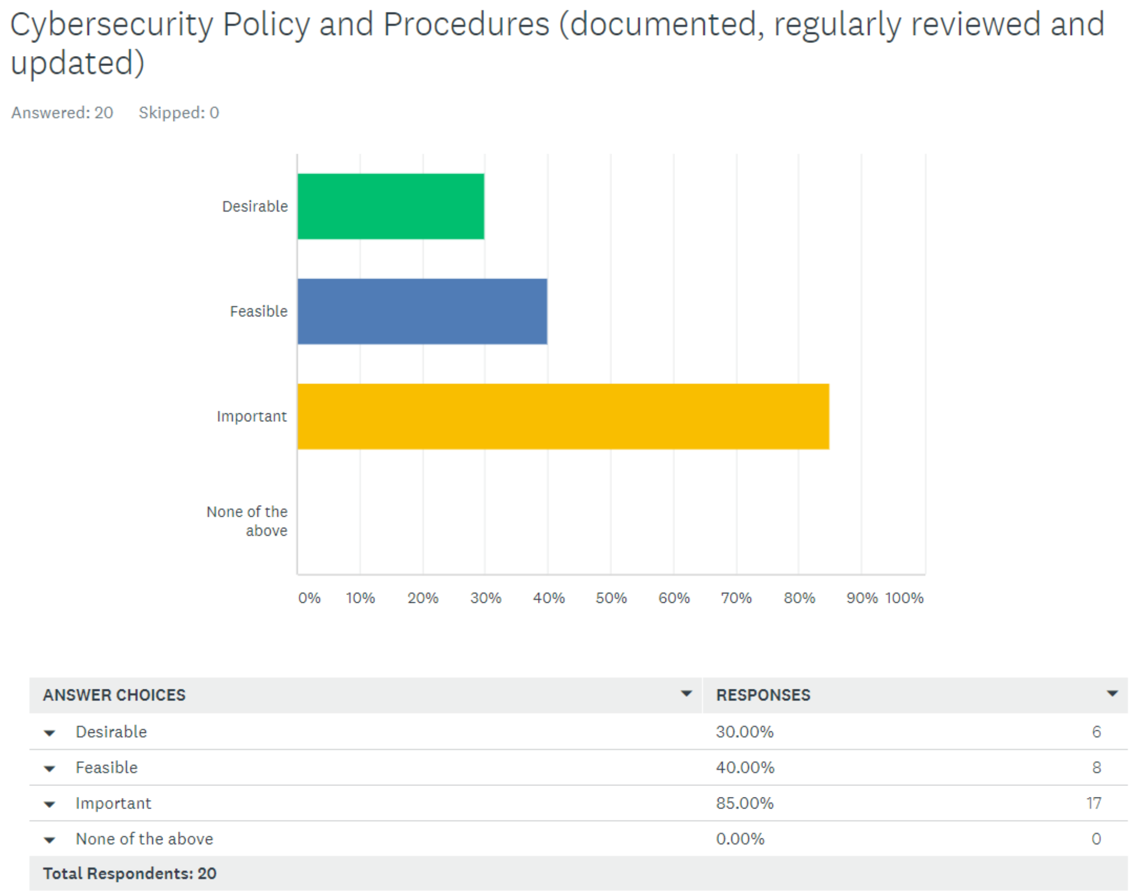
Answered: 20 Skipped: 0

ANSWER CHOICES	RESPONSES	
Desirable	45.00%	9
Feasible	50.00%	10
Important	70.00%	14
None of the above	0.00%	0
Total Respondents: 20		

R2 Q5:

Figure 36

Survey Round 2, Question 5 Results



Cybersecurity Policy and Procedures (documented, regularly reviewed and updated)

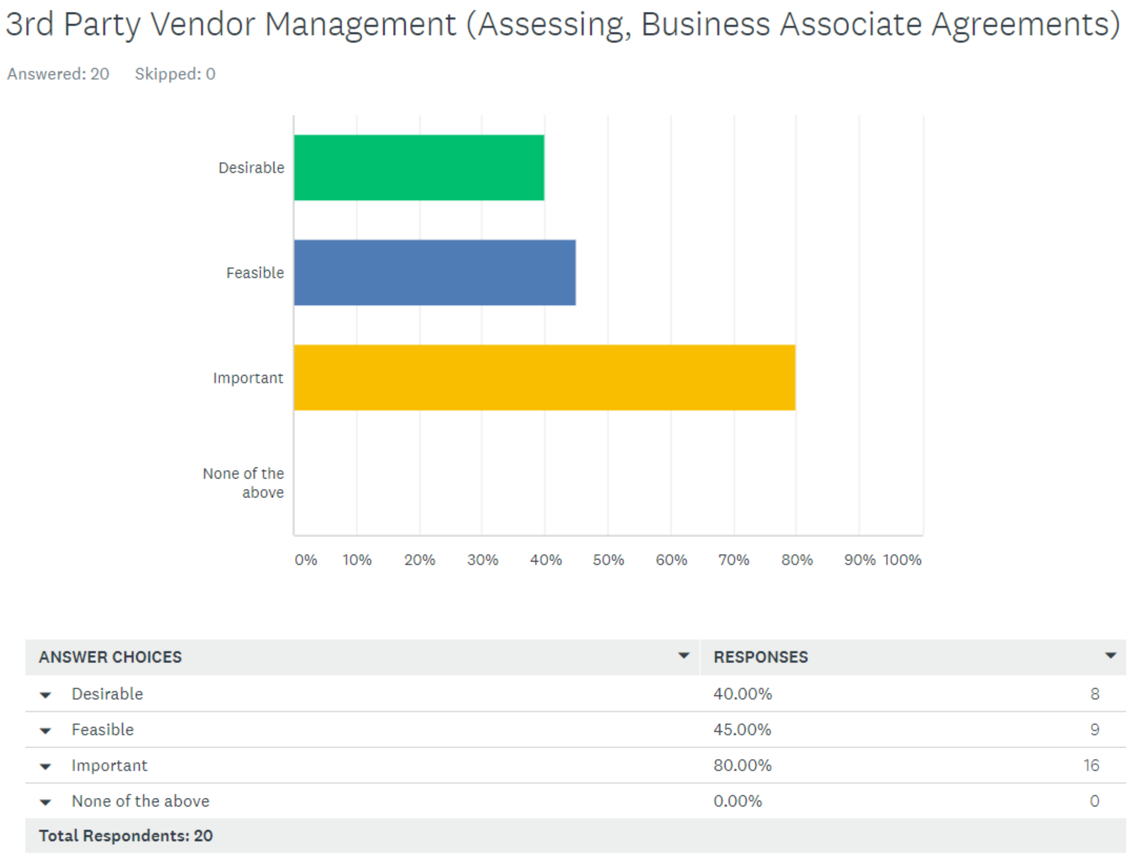
Answered: 20 Skipped: 0

ANSWER CHOICES	RESPONSES	
Desirable	30.00%	6
Feasible	40.00%	8
Important	85.00%	17
None of the above	0.00%	0
Total Respondents: 20		

R2 Q6:

Figure 37

Survey Round 2, Question 6 Results



3rd Party Vendor Management (Assessing, Business Associate Agreements)

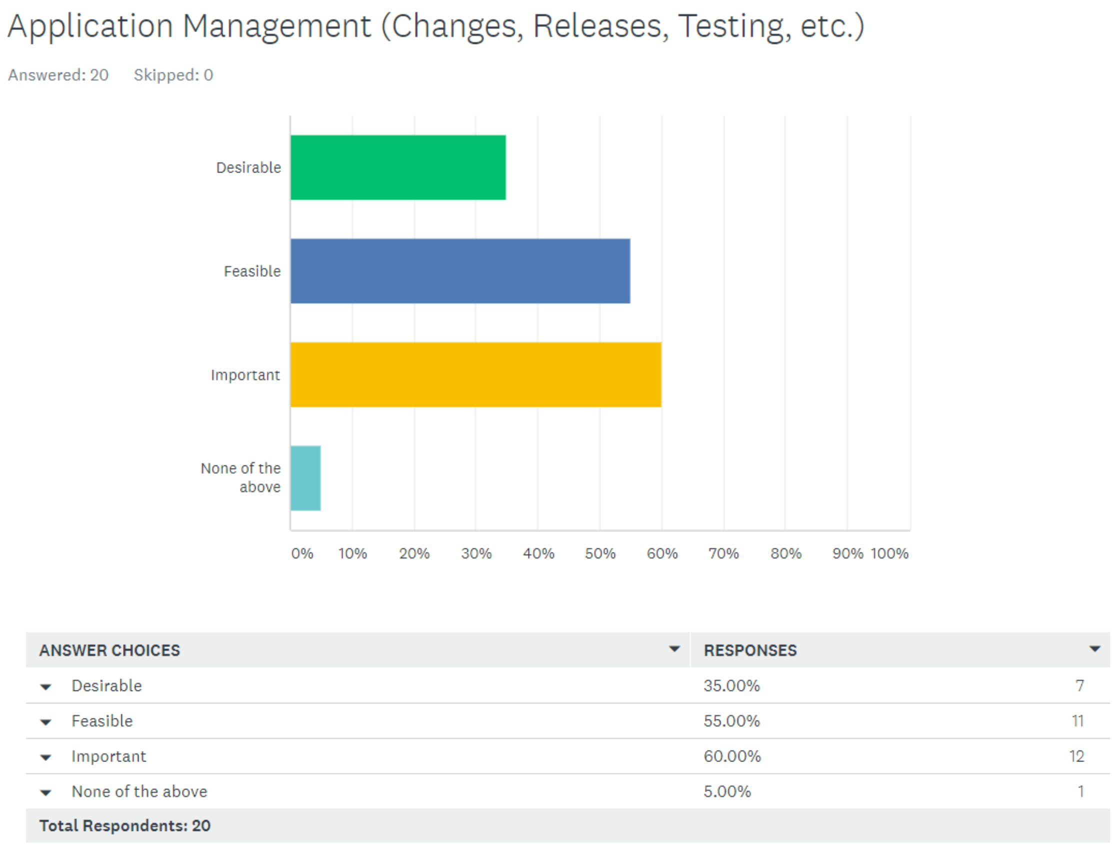
Answered: 20 Skipped: 0

ANSWER CHOICES	RESPONSES	
Desirable	40.00%	8
Feasible	45.00%	9
Important	80.00%	16
None of the above	0.00%	0
Total Respondents: 20		

R2 Q7:

Figure 38

Survey Round 2, Question 7 Results



Application Management (Changes, Releases, Testing, etc.)

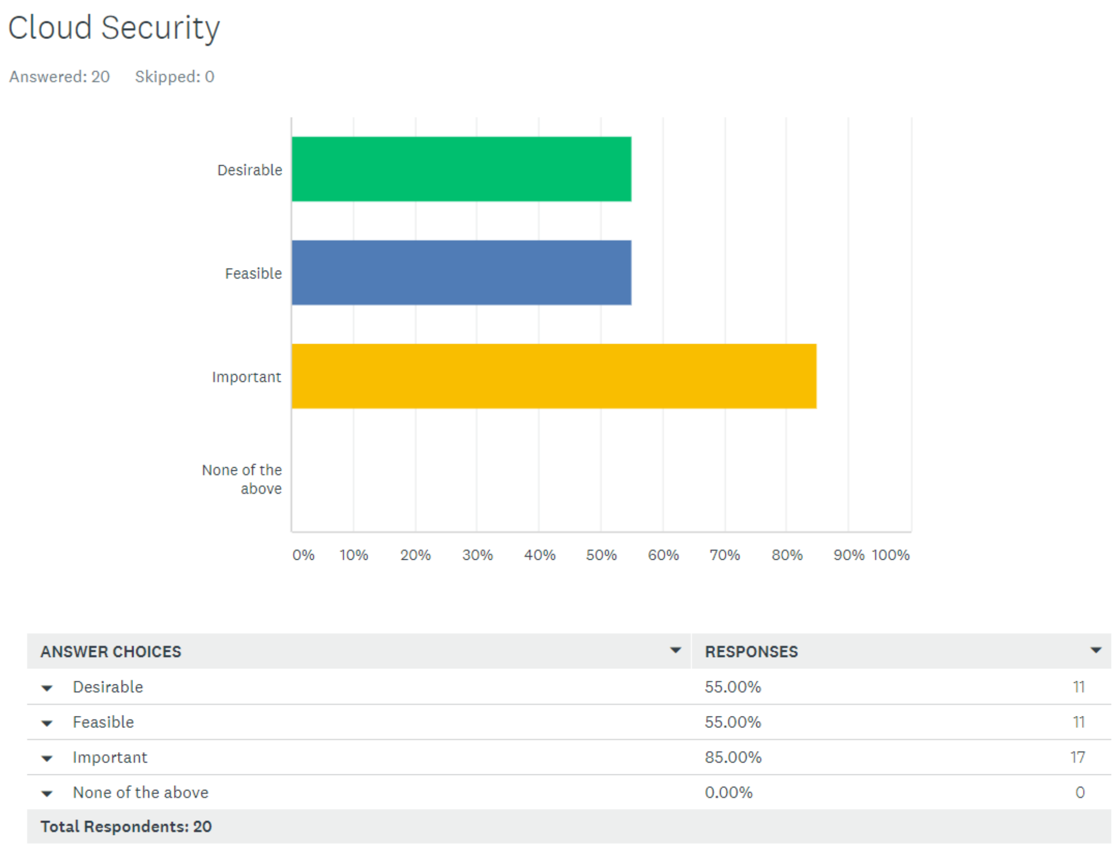
Answered: 20 Skipped: 0

ANSWER CHOICES	RESPONSES	
Desirable	35.00%	7
Feasible	55.00%	11
Important	60.00%	12
None of the above	5.00%	1
Total Respondents: 20		

R2 Q8:

Figure 39

Survey Round 2, Question 8 Results



Cloud Security

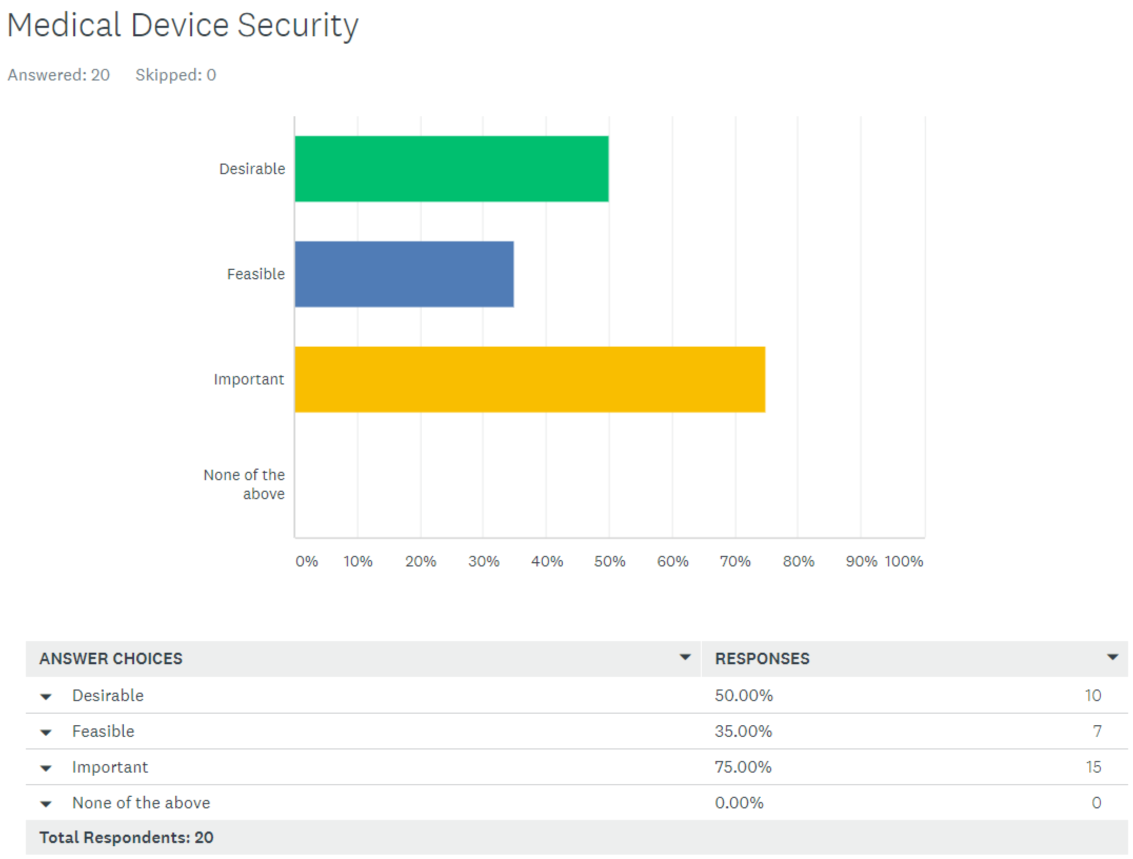
Answered: 20 Skipped: 0

ANSWER CHOICES	RESPONSES	
Desirable	55.00%	11
Feasible	55.00%	11
Important	85.00%	17
None of the above	0.00%	0
Total Respondents: 20		

R2 Q9:

Figure 40

Survey Round 2, Question 9 Results



Medical Device Security

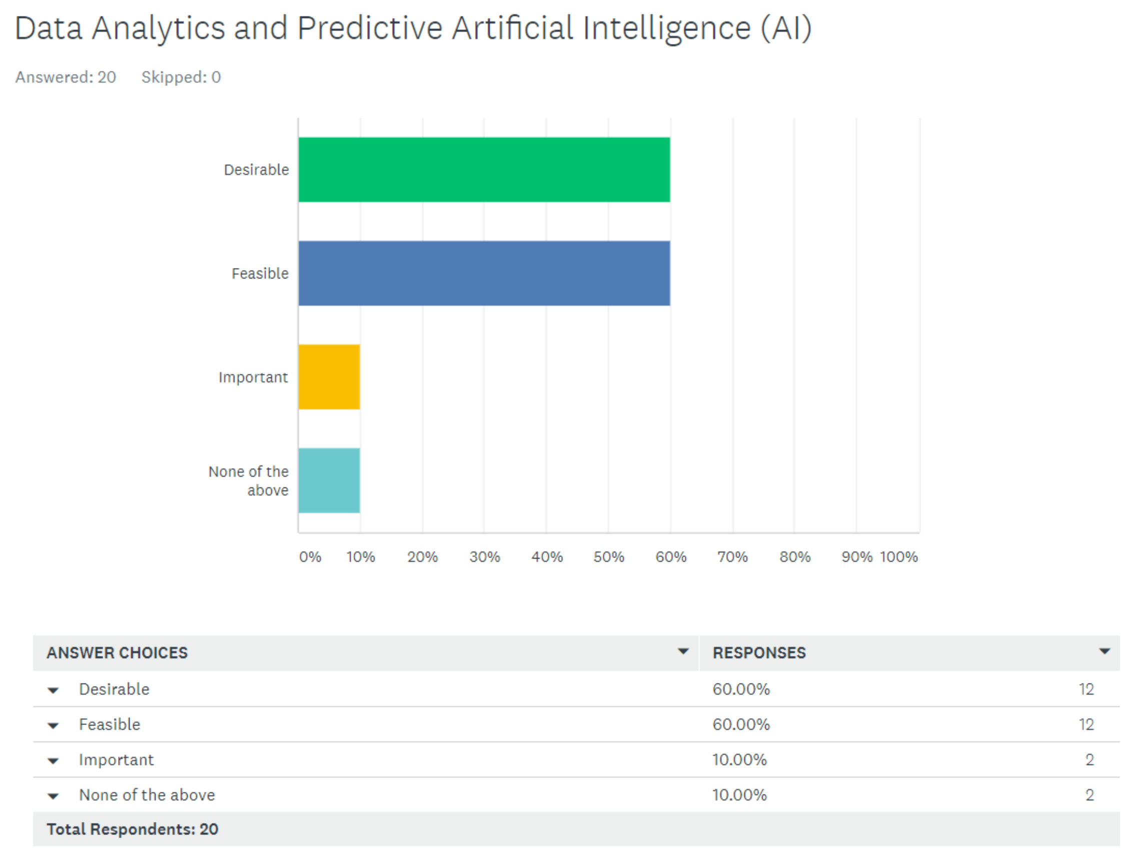
Answered: 20 Skipped: 0

ANSWER CHOICES	RESPONSES	
Desirable	50.00%	10
Feasible	35.00%	7
Important	75.00%	15
None of the above	0.00%	0
Total Respondents: 20		

R2 Q10:

Figure 41

Survey Round 2, Question 10 Results



Data Analytics and Predictive Artificial Intelligence (AI)

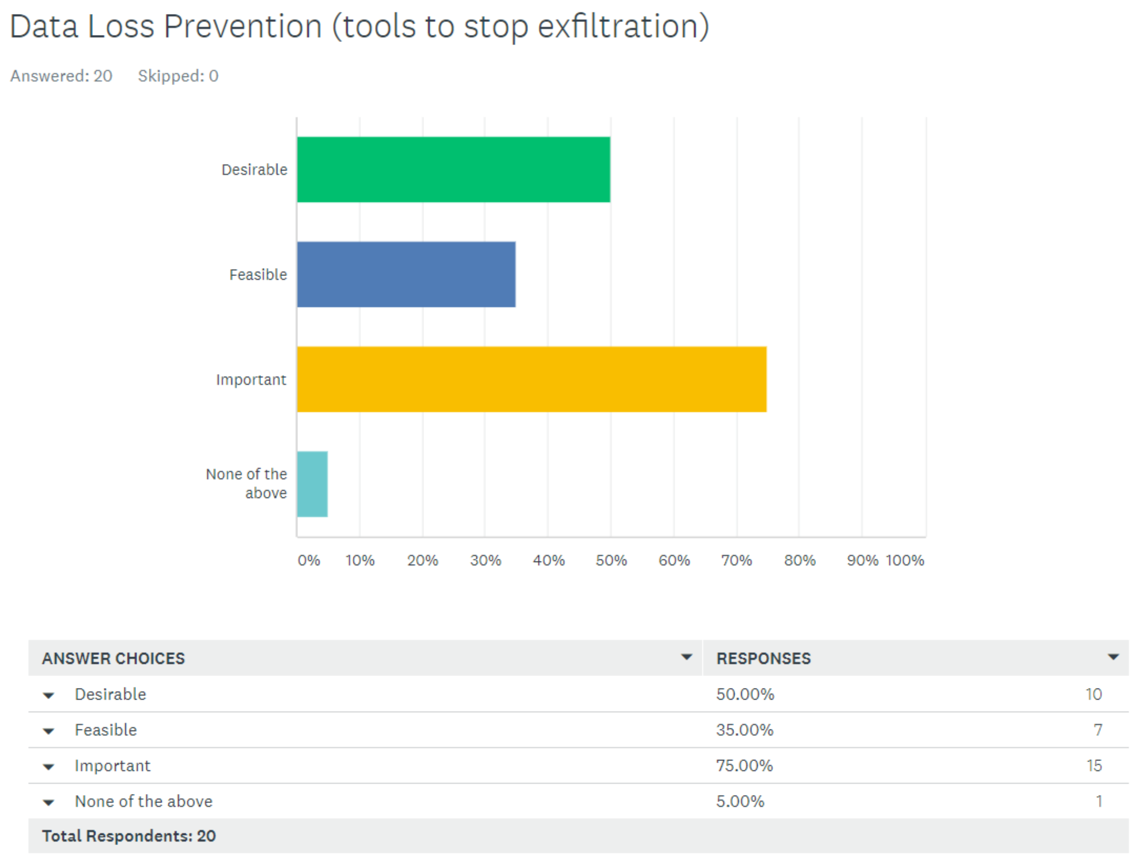
Answered: 20 Skipped: 0

ANSWER CHOICES	RESPONSES	
Desirable	60.00%	12
Feasible	60.00%	12
Important	10.00%	2
None of the above	10.00%	2
Total Respondents: 20		

R2 Q11:

Figure 42

Survey Round 2, Question 11 Results



Data Loss Prevention (tools to stop exfiltration)

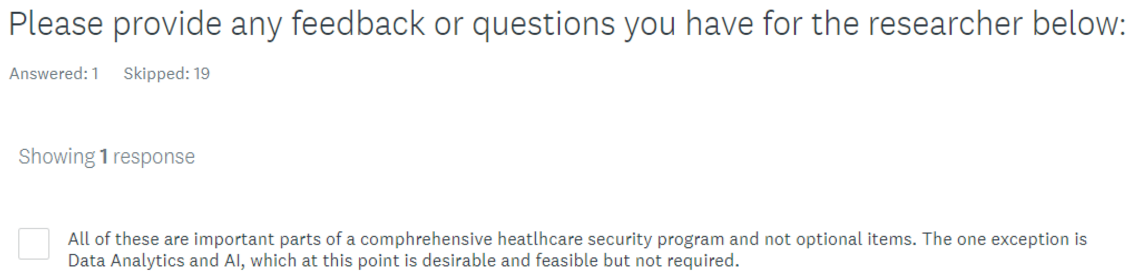
Answered: 20 Skipped: 0

ANSWER CHOICES	RESPONSES	
Desirable	50.00%	10
Feasible	35.00%	7
Important	75.00%	15
None of the above	5.00%	1
Total Respondents: 20		

R2 Q12:

Figure 43

Survey Round 2, Question 12 Results



Please provide any feedback or questions you have for the researcher below:

Answered: 1 Skipped: 19

Showing **1** response

□ All of these are important parts of a comphrehensive heatlhcare security program and not optional items. The one exception is Data Analytics and AI, which at this point is desirable and feasible but not required.

Appendix F: Round 3 Survey Questions

The following email was sent to all participants to let them know that the final round of the survey is coming:

> “Thank you for your responses from the first two rounds of the surveys for the Delphi study. The information was utilized to create Round 3 of the survey. The link for Round 3 of the survey will be emailed via Survey Monkey within the next few days. Please respond within 48 hours of the receipt of the email. Thank you again!”

Instructions for Q1:

Included below are the top risk remediation strategies based on desirability, feasibility, and importance from the results of the second round of the survey. Please rank from 1 (highest) to 13 (lowest) in order of desirability, feasibility, and importance by dropping and dragging into the correct prioritized order:

Establishing a Cybersecurity Program

Strong Passwords and Multifactor Authentication

Cybersecurity Hygiene (backups, patching, recovery testing, etc.)

Risk Analysis and Risk Management Plan

Cybersecurity Awareness and Training

Continuous Monitoring of Critical Systems

Incident Response Plans and Testing

Intrusion Detection and Prevention Tools

Identity Access Management

Governance (Executive and board level engagement, alignment to operations)

Cybersecurity Policy and Procedures (documented, regularly reviewed and updated)

3rd Party Vendor Management (Assessing, Business Associate Agreements)

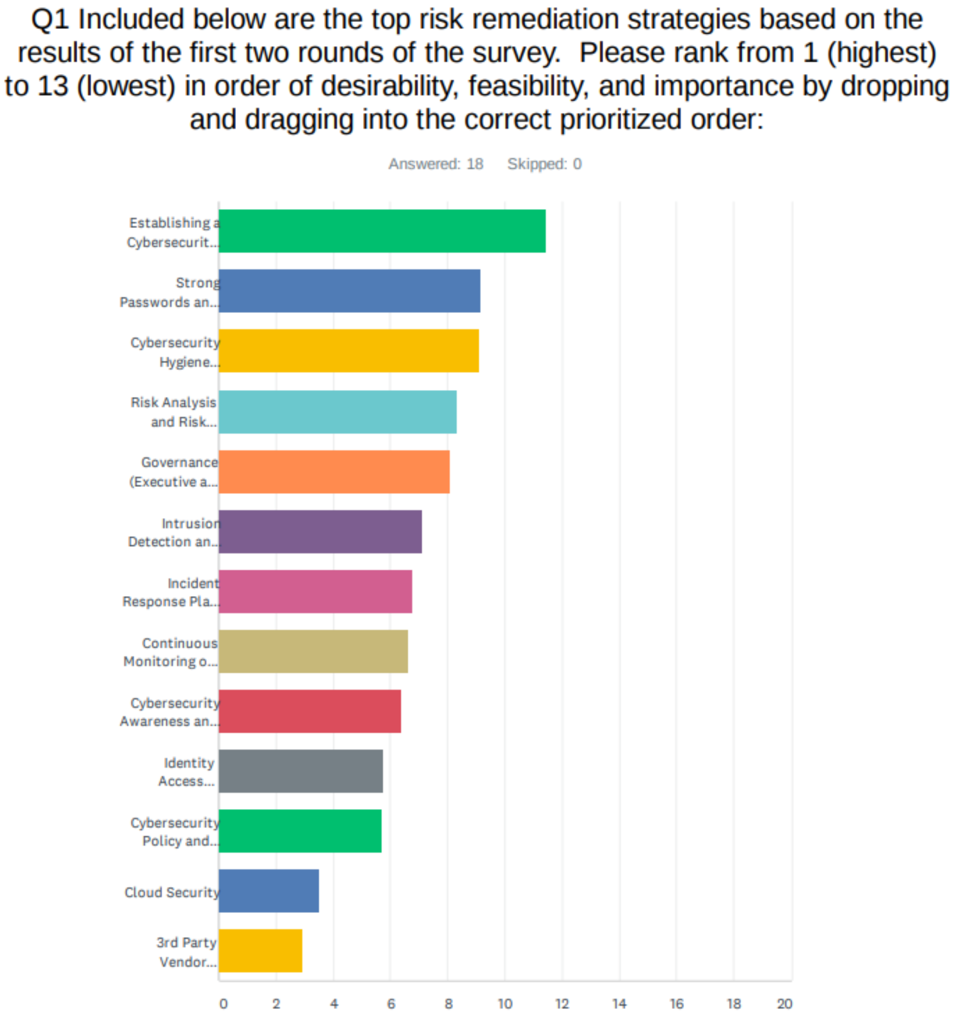
Cloud Security

Q2—Please provide any feedback or questions you have for the researcher below:

Appendix G: Round 3 Survey Responses

Figure 44

Survey Round 3, Question 1 Results

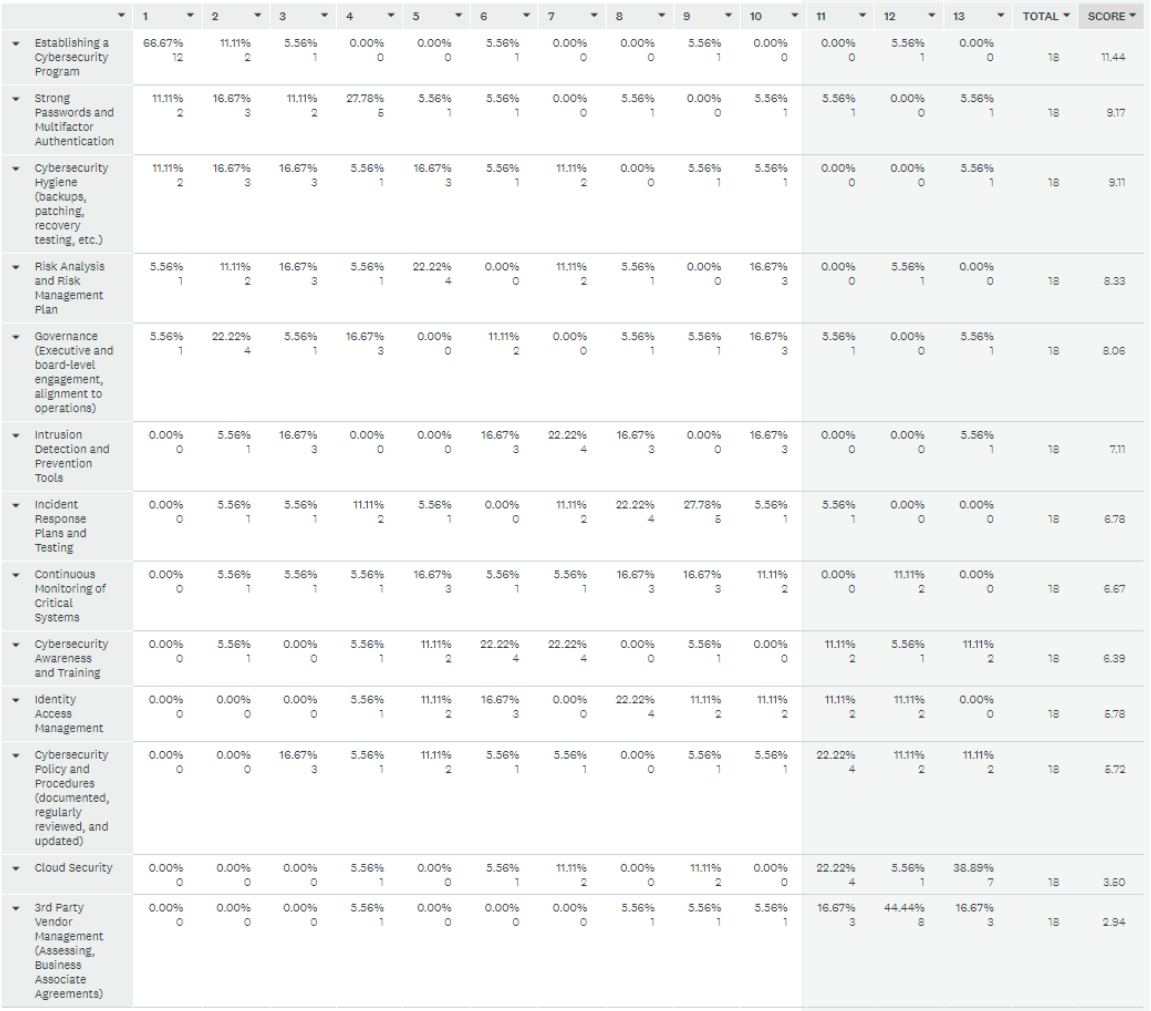


Q1 Included below are the top risk remediation strategies based on the results of the first two rounds of the survey. Please rank from 1 (highest) to 13 (lowest) in order of desirability, feasibility, and importance by dropping and dragging into the correct prioritized order:

Answered: 18 Skipped: 0

Figure 45

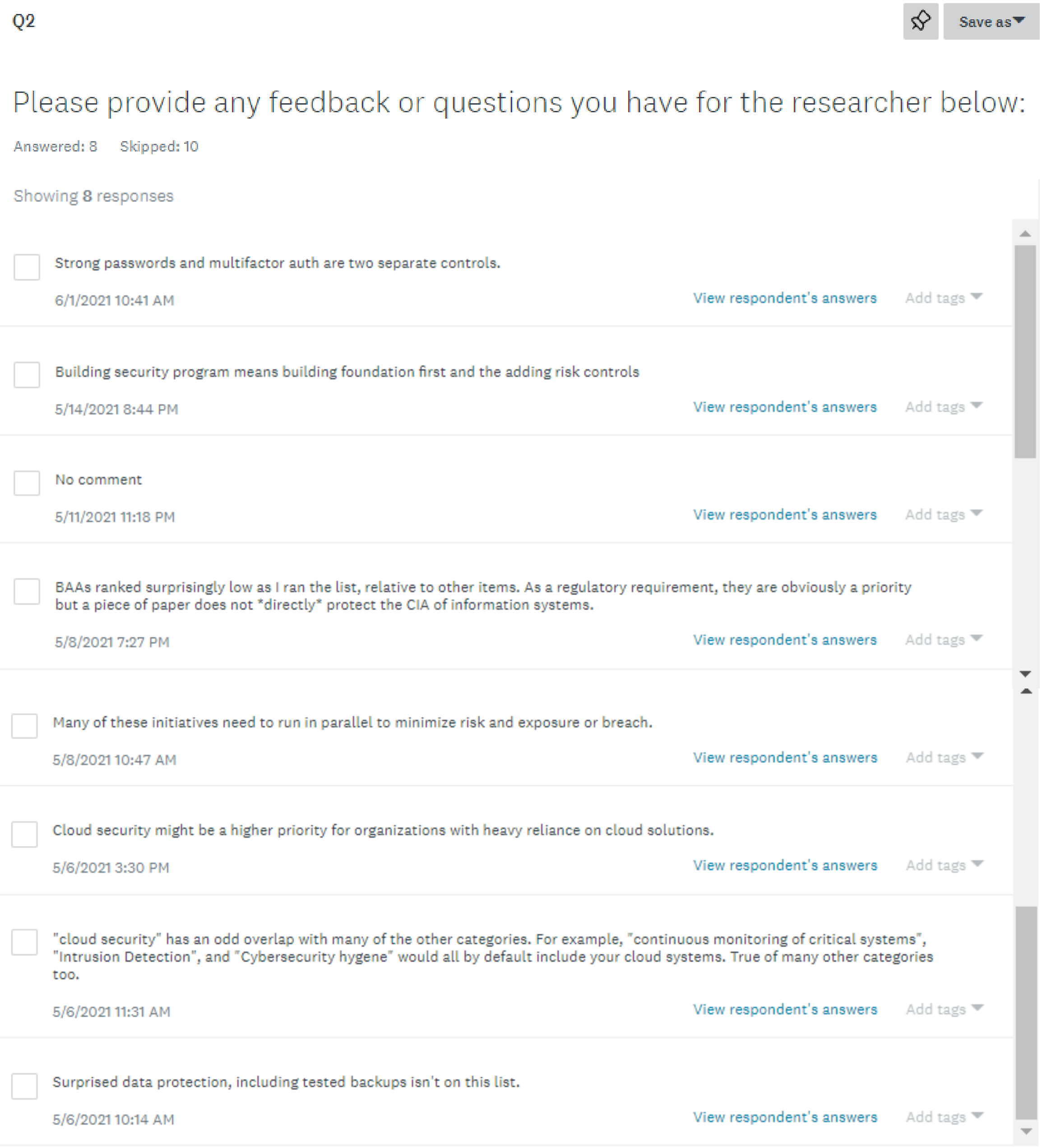
Survey Round 3, Question 1 Data



	1	2	3	4	5	6	7	8	9	10	11	12	13	TOTAL	SCORE
Establishing a Cybersecurity Program	66.67% 12	11.11% 2	5.56% 1	0.00% 0	0.00% 0	5.56% 1	0.00% 0	0.00% 0	5.56% 1	0.00% 0	0.00% 0	5.56% 1	0.00% 0	18	11.44
Strong Passwords and Multifactor Authentication	11.11% 2	16.67% 3	11.11% 2	27.78% 5	5.56% 1	5.56% 1	0.00% 0	5.56% 1	0.00% 0	5.56% 1	5.56% 1	0.00% 0	5.56% 1	18	9.17
Cybersecurity Hygiene (backups, patching, recovery testing, etc.)	11.11% 2	16.67% 3	16.67% 3	5.56% 1	16.67% 3	5.56% 1	11.11% 2	0.00% 0	5.56% 1	5.56% 1	0.00% 0	0.00% 0	5.56% 1	18	9.11
Risk Analysis and Risk Management Plan	5.56% 1	11.11% 2	16.67% 3	5.56% 1	22.22% 4	0.00% 0	11.11% 2	5.56% 1	0.00% 0	16.67% 3	0.00% 0	5.56% 1	0.00% 0	18	8.33
Governance (Executive and board-level engagement, alignment to operations)	5.56% 1	22.22% 4	5.56% 1	16.67% 3	0.00% 0	11.11% 2	0.00% 0	5.56% 1	5.56% 1	16.67% 3	5.56% 1	0.00% 0	5.56% 1	18	8.06
Intrusion Detection and Prevention Tools	0.00% 0	5.56% 1	16.67% 3	0.00% 0	0.00% 0	16.67% 3	22.22% 4	16.67% 3	0.00% 0	16.67% 3	0.00% 0	0.00% 0	5.56% 1	18	7.11
Incident Response Plans and Testing	0.00% 0	5.56% 1	5.56% 1	11.11% 2	5.56% 1	0.00% 0	11.11% 2	22.22% 4	27.78% 5	5.56% 1	5.56% 1	0.00% 0	0.00% 0	18	6.78
Continuous Monitoring of Critical Systems	0.00% 0	5.56% 1	5.56% 1	5.56% 1	16.67% 3	5.56% 1	5.56% 1	16.67% 3	16.67% 3	11.11% 2	0.00% 0	11.11% 2	0.00% 0	18	6.67
Cybersecurity Awareness and Training	0.00% 0	5.56% 1	0.00% 0	5.56% 1	11.11% 2	22.22% 4	22.22% 4	0.00% 0	5.56% 1	0.00% 0	11.11% 2	5.56% 1	11.11% 2	18	6.39
Identity Access Management	0.00% 0	0.00% 0	0.00% 0	5.56% 1	11.11% 2	16.67% 3	0.00% 0	22.22% 4	11.11% 2	11.11% 2	11.11% 2	11.11% 2	0.00% 0	18	5.78
Cybersecurity Policy and Procedures (documented, regularly reviewed, and updated)	0.00% 0	0.00% 0	16.67% 3	5.56% 1	11.11% 2	5.56% 1	5.56% 1	0.00% 0	5.56% 1	5.56% 1	22.22% 4	11.11% 2	11.11% 2	18	5.72
Cloud Security	0.00% 0	0.00% 0	0.00% 0	5.56% 1	0.00% 0	5.56% 1	11.11% 2	0.00% 0	11.11% 2	0.00% 0	22.22% 4	5.56% 1	38.89% 7	18	3.50
3rd Party Vendor Management (Assessing, Business Associate Agreements)	0.00% 0	0.00% 0	0.00% 0	5.56% 1	0.00% 0	0.00% 0	0.00% 0	5.56% 1	5.56% 1	5.56% 1	16.67% 3	44.44% 8	16.67% 3	18	2.94

Figure 46

Survey Round 3, Question 2 Results



Q2

Please provide any feedback or questions you have for the researcher below:

Answered: 8 Skipped: 10

Showing **8** responses

□ Strong passwords and multifactor auth are two separate controls.

6/1/2021 10:41 AM

□ Building security program means building foundation first and the adding risk controls

5/14/2021 8:44 PM

□ No comment

5/11/2021 11:18 PM

□ BAAs ranked surprisingly low as I ran the list, relative to other items. As a regulatory requirement, they are obviously a priority but a piece of paper does not *directly* protect the CIA of information systems.

5/8/2021 7:27 PM

□ Many of these initiatives need to run in parallel to minimize risk and exposure or breach.

5/8/2021 10:47 AM

□ Cloud security might be a higher priority for organizations with heavy reliance on cloud solutions.

5/6/2021 3:30 PM

□ "cloud security" has an odd overlap with many of the other categories. For example, "continuous monitoring of critical systems", "Intrusion Detection", and "Cybersecurity hygene" would all by default include your cloud systems. True of many other categories too.

5/6/2021 11:31 AM

□ Surprised data protection, including tested backups isn't on this list.

5/6/2021 10:14 AM

Appendix H: Data Analysis (Coding Tables)

Round 1 – Initial Codes and Emerging Categories

Initial codes included for the survey questions in round 1 for questions 2-19 are the strategies that came from the literature review. The examples from data collected during the survey show the scores calculated from the participant responses. The notes from analysis are included and indicate which strategies will be included in the round 2 survey questions. The responses from the open text question for question 20 are included below. (For additional details, please reference Table 5 *Round 1 Survey—Summary of Results).*

Initial Code	**Data Collected – Scores and Comments**	**Analytic Notes on Emerging Categories**
Cybersecurity Awareness and Training (Q2)	Survey Response Score for "All of the Above": 16	Higher score – will be included in the Round 2 Survey questions.
Strong Passwords and Multifactor Authentication (Q3)	Survey Response Score for "All of the Above": 15	Higher score – will be included in the Round 2 Survey questions.
Establishing a Cybersecurity Program (Q4)	Survey Response Score for "All of the Above": 16	Higher score – will be included in the Round 2 Survey questions.
Culture of Risk Awareness (Q5)	Survey Response Score for "All of the Above": 13	Not to be included in the Round 2 Survey questions – the score of 13 is borderline, I considered the scores for desirable, feasible and important and determined to not include this code Round 2.
Monitoring Mobile Devices and Social Media (Q6)	Survey Response Score for "All of the Above": 9	Not to be included in the Round 2 Survey questions
Risk Analysis and Risk Management Plans (Q7)	Survey Response Score for "All of the Above": 15	Higher score – will be included in the Round 2 Survey questions.
Cybersecurity Hygiene (backups, patching, etc.) (Q8)	Survey Response Score for "All of the Above": 15	Higher score – will be included in the Round 2 Survey questions.
Built-in Upfront Security Mechanisms (Q9)	Survey Response Score for "All of the Above": 9	Not to be included in the Round 2 Survey questions
Cyber Insurance (Q10)	Survey Response Score for "All of the Above": 8	Not to be included in the Round 2 Survey questions
3- to 5-Year Cybersecurity Plan (Q11)	Survey Response Score for "All of the Above": 8	Not to be included in the Round 2 Survey questions
Asset Management (Inventory of Software and Hardware) (Q12)	Survey Response Score for "All of the Above": 7	Not to be included in the Round 2 Survey questions
Continuous Monitoring of Critical Systems (Q13)	Survey Response Score for "All of the Above": 13	Higher score – will be included in the Round 2 Survey questions.
Incident Response Plans and Testing (Q14)	Survey Response Score for "All of the Above": 13	Higher score – will be included in the Round 2 Survey questions.
Encryption of Data at Rest and In Transit (Q15)	Survey Response Score for "All of the Above": 8	Not to be included in the Round 2 Survey questions

Intrusion Detection and Prevention Tools (Q16)	Survey Response Score for “All of the Above”: 13	Higher score – will be included in the Round 2 Survey questions.
Backup and Recovery Testing (Q17)	Survey Response Score for “All of the Above”: 13	Higher score – will be included in the Round 2 Survey questions.
Recruiting, Training and Retraining Cybersecurity Staff (Q18)	Survey Response Score for “All of the Above”: 10	Not to be included in the Round 2 Survey questions
Internal Stakeholder Alignment with Cybersecurity Strategies (Q19)	Survey Response Score for “All of the Above”: 11	Not to be included in the Round 2 Survey questions
The remaining codes evolved from the participants responses to question 20: **“What additional cybersecurity risk mitigation strategies are desirable, feasible, and important in your perspective that is not included in the list above?” (Q20)**		
Identity Access Authorization Control	Q20 Open Text Comment “Identity access and authorization control” (P10)	Category to be added to Round 2: Identity Access Management Strategy
Identity Management Vendor Account Controls Privileged Account Controls	Q20 Open Text Comment “Identity Management, vendor account controls, privileged account controls” (P11)	Category to be added to Round 2: Identity Access Management Strategy
External Site Access Multifactor Authentication Privileged Account Access Monitoring	Q20 Open Text Comment “Restricting access to external sites (web filtering, personal email apps), multi-factor authentication for remote access, privileged account access monitoring.” (P15)	Category to be added to Round 2: Identity Access Management Strategy
Alignment Governance	Q20 Open Text Comment “Alignment to continuity of operations” (P2)	Category to be added to Round 2: Governance (executive and board-level engagement, alignment to operations)
Executive Board of Directors Governance	Q20 Open Text Comment “Executive and Board of Directors engagement” (P16)	Category to be added to Round 2: Governance (executive and board-level engagement, alignment to operations)
Cybersecurity Framework	Q20 Open Text Comment “Having a Cyber-Security Framework is Desirable” (P12)	Category to be added to Round 2: Cybersecurity Frameworks (i.e., NIST, HIPAA, ISO)
Cybersecurity Policy and Procedures	Q20 Open Text Comment “Having a Cyber-Security Framework is Desirable” (P12)	Category to be added to Round 2: Cybersecurity Policy and Procedures (documented, regularly reviewed, and updated)
Application Management	Q20 Open Text Comment	Category to be added to Round 2: Third-Party Vendor Management

Third-Party Vendor Management	“Effective Application and 3rd party solution management” (P13)	(assessing, business associate agreements)
Vendor Assessment Management	Q20 Open Text Comment “3rd Party Vendor Assessment | Management” (P17)	Category to be added to Round 2: Third-Party Vendor Management (assessing, business associate agreements)
Application Management	Q20 Open Text Comment “Effective Application and 3rd party solution management” (P13)	Category to be added to Round 2: Application Management (changes, releases, testing, etc.)
Cloud Security	Q20 Open Text Comment “Cloud Security” (P21)	Category to be added to Round 2: Cloud Security
Medical Device Security	Q20 Open Text Comment “Medical Device Security” (P5)	Category to be added to Round 2: Medical Device Security
Data Analytics Predictive AI	Q20 Open Text Comment “Data Analytics and Predictive AI” (P20)	Category to be added to Round 2: Data Analytics and Predictive Artificial Intelligence (AI)
Data Loss Prevention	Q20 Open Text Comment “Data loss prevention is desirable, feasible and important for PII and PHI protection.” (P7)	Category to be added to Round 2: Data Loss Prevention (tools to stop exfiltration)
Logging Monitoring	Q20 Open Text Comment “Log and Network Flow collection, SIEM, SOC” (P24)	Not added to Round 2, already covered in Round 1
Monitoring	Q20 Open Text Comment “24x7 monitoring, alerting, and response capability.” (P27)	Not added to Round 2, already covered in Round 1
Monitoring Risk Analysis	Q20 Open Text Comment “Threat Intelligence, Automation (a.k.a. SOAR), Continuous Penetration Testing, Evaluation of Security Systems/Applications” (P8)	Not added to Round 2, already covered in Round 1
Recruiting	Q20 Open Text Comment “Most of these were all of the above. The only reason I marked recruiting as Desirable is because you could theoretically outsource that component.” (P19)	Not added to Round 2, comment about why participant answered the way they did. Recruiting is not a new category, already covered in Round 1

Round 2
Categories and Emerging Themes

The new categories uncovered in round 1 were used for questions in round 2 to get additional insight from the participants. The participants were provided a list of eight strategies (codes) to prioritize for Q1 in round 2. And round 2 Q2-Q11 included the newly identified strategies (codes) that the participants provided in the round 1 Q20 open text responses. For round 2 Q12, there was one open text response. (For additional details, please reference Table 6 *Round 2 Survey—Summary of Results Q2 through Q11).*

Initial Code	**Secondary Code/Category**	**Analytic Notes on Emerging Themes**
Cybersecurity Awareness and Training (Q1)	Q1 Survey Ranked Result: 6.55	Potential emerging top three strategy.
Strong Passwords and Multifactor Authentication (Q1)	Q1 Survey Ranked Result: 5.25	Potential emerging top three strategy.
Establishing a Cybersecurity Program (Q1)	Q1 Survey Ranked Result: 5.20	Potential emerging top three strategy.
Risk Analysis and Risk Management Plan (Q1)	Q1 Survey Ranked Result: 4.80	Potential emerging top three strategy.
Cybersecurity Hygiene (backups, patching, recovery testing, etc.) (Q1)	Q1 Survey Ranked Result: 3.95	Not potentially an emerging top three strategy due to low score.
Continuous Monitoring of Critical Systems(Q1)	Q1 Survey Ranked Result: 3.65	Not potentially an emerging top three strategy due to low score.
Incident Response Plans and Testing (Q1)	Q1 Survey Ranked Result: 3.55	Not potentially an emerging top three strategy due to low score.
Intrusion Detection and Prevention Tools (Q1)	Q1 Survey Ranked Result: 3.05	Not potentially an emerging top three strategy due to low score.
Q2-Q12 were the additional strategies (codes) identified by the participants in Round 1. The participants were asked if each was desirable, feasible, important and any combination was possible. These ten strategies were scored similar to the Round 1 questions.		
Identity Access Management (Q2)	Survey Response Score: 40	Higher score – will be included in the Round 3 survey questions.
Governance (Executive and board-level engagement, alignment to operations) (Q3)	Survey Response Score: 33	Higher score – will be included in the Round 3 survey questions.
Cybersecurity Frameworks (i.e., NIST, HIPAA, ISO) (Q4)	Survey Response Score: 33	Not to be included in the Round 3 Survey questions. Although a higher score of 33, I determined there was an overlapping strategy from Round 1, Establishing a Cybersecurity Program.

		Removed from the codes going to Round 3 to avoid duplication.
Cybersecurity Policy and Procedures (documented, regularly reviewed and updated) (Q5)	Survey Response Score: 31	Higher score – will be included in the Round 3 survey questions.
Third-Party Vendor Management (Assessing, Business Associate Agreements) (Q6)	Survey Response Score: 31	Higher score – will be included in the Round 3 survey questions.
Application Management (Changes, Releases, Testing, etc.) (Q7)	Survey Response Score: 30	Not to be included in the Round 3 survey questions.
Cloud Security (Q8)	Survey Response Score: 39	Higher score – will be included in the Round 3 survey questions.
Medical Device Security (Q9)	Survey Response Score: 32	Not to be included in the Round 3 survey questions.
Data Analytics and Predictive Artificial Intelligence (AI) (Q10)	Survey Response Score: 30	Not to be included in the Round 3 survey questions, also considering the response in Q12.
Data Loss Prevention (tools to stop exfiltration) (Q11)	Survey Response Score: 32	Not to be included in the Round 3 survey questions.
Please provide any feedback or questions you have for the researcher below (Q12)	"All of these are important parts of a comprehensive healthcare security program and not optional items. The one exception is Data Analytics and AI which are desirable and feasible, but not required." (P15)	Excellent observation that all items are important and not optional. The survey is trying to determine how experts rank these controls. Also, the Data Analytics and AI strategy was added from round 1 response.

Round 3
Themes

The final round of survey questions consisted of Q1 which was a list of thirteen strategies to be prioritized by the participants. The table below shows the strategy scores in ranking order, highest to lowest. Q2 was the final chance for participants to provide feedback or ask questions and there were eight responses.

Theme	**Data Collected – Scores and Comments**	**Key Codes and Categories Related to the Themes**
Establishing a Cybersecurity Program (Q1)	Survey Response Score: 11.44	One of the top three strategies identified.
Strong Passwords and Multifactor Authentication (Q1)	Survey Response Score: 9.17	One of the top three strategies identified.

Cybersecurity Hygiene (backups, patching, recovery testing, etc.) (Q1)	Survey Response Score: 9.11	One of the top three strategies identified.
Risk Analysis and Risk Management Plan (Q1)	Survey Response Score: 8.33	Not one of the top three strategies identified.
Cybersecurity Awareness and Training (Q1)	Survey Response Score: 8.06	Not one of the top three strategies identified.
Continuous Monitoring of Critical Systems (Q1)	Survey Response Score: 7.11	Not one of the top three strategies identified.
Incident Response Plans and Testing (Q1)	Survey Response Score: 6.78	Not one of the top three strategies identified.
Intrusion Detection and Prevention Tools (Q1)	Survey Response Score: 6.67	Not one of the top three strategies identified.
Identity Access Management (Q1)	Survey Response Score: 6.39	Not one of the top three strategies identified.
Governance (Executive and board level engagement, alignment to operations) (Q1)	Survey Response Score: 5.78	Not one of the top three strategies identified.
Cybersecurity Policy and Procedures (documented, regularly reviewed and updated) (Q1)	Survey Response Score: 5.72	Not one of the top three strategies identified.
3rd Party Vendor Management (Assessing, Business Associate Agreements) (Q1)	Survey Response Score: 3.60	Not one of the top three strategies identified.
Cloud Security (Q1)	Survey Response Score: 2.94	Not one of the top three strategies identified.
I provided a final opportunity in the final round of the surveys for the participants to provide their feedback and questions. **“Please provide any feedback or questions you have for the researcher below (Q2).”**		
Authentication	“Strong passwords and multifactor auth are two separate controls.” (P2)	I agree with this comment, however, both surround authentication controls and are commonly implemented together. Authentication controls are seen as one of the top three most desirable, feasible and important strategies for organizations to implement.
Establishing a Security Program	“Building security program means building foundation first and the adding risk controls” (P4)	The research agrees with this comment, and without a strong foundation, the controls will not be organized and standard across the organization. This top three strategy is key for an organization to properly implement the required controls.
NA	“No comment” (P6)	NA
3rd Party Vendor Management	“BAAs ranked surprisingly low as I ran the list, relative to	As further explanation, a BAA is a Business Associate Agreement and is

	other items. As a regulatory requirement, they are obviously a priority but a piece of paper does not *directly* protect the CIA of information systems.” (P9)	related to 3rd Party Vendor Management. This did rank low in the list. I understand the comment that a piece of paper does nothing to protect the confidentiality, integrity, and availability of the organizations data. However, without BAAs for all vendors, the vendors might not protect the organizations data and legal agreements to do so would be important if the vendor causes a breach.
Establishing a Security Program	“Many of these initiatives need to run in parallel to minimize risk and exposure or breach.” (P10)	I also agree with this comment. Knowing which items should be required to be in place (i.e., which are the most desirable, feasible and important) will help ensure data is protected. The security program should be designed with the needs of the organization and those overlapping areas identified in the program.
Cloud Security	“Cloud security might be a higher priority for organizations with heavy reliance on cloud solutions.” (P15)	I agree with this comment, however, for organizations with no reliance on cloud implementations, it would be not required. A security program designed for the organizational needs should take into consideration what is required and what is not.
Establishing a Security Program	“"cloud security" has an odd overlap with many of the other categories. For example, "continuous monitoring of critical systems", "Intrusion Detection", and "Cybersecurity hygiene" would all by default include your cloud systems. True of many other categories too.” (P16)	I agree with this very insightful comment. The security program designed for the organizational needs should take into consideration what are the overlapping controls.
Cybersecurity Hygiene (backups, patching, recovery testing, etc.) (Q1)	“Surprised data protection, including tested backups isn't on this list.” (P18)	I merged backups and recovery testing with the Cybersecurity Hygiene strategy. This was identified as one of the top three strategies. Also, the term data protection is generic and can be interpreted to mean many of the other items on the list.