JOURNAL OF BUSINESS, TECHNOLOGY & LEADERSHIP
SCHOOL OF BUSINESS AND TECHNOLOGY – COLLEGE OF ADULT AND GRADUATE STUDIES
COLORADO CHRISTIAN UNIVERSITY PEER REVIEWED PUBLICATION
VOLUME 4 NUMBER 2: Spring 2022 PAGES 1-13

Ransomware Attacks on the Healthcare Industry

Dr. William Triplett
Technology and Healthcare Executive | Faculty | Advisory Board

Abstract
The increase of cybersecurity threats poses a significant risk to the healthcare industry, specifically, healthcare organizations, pharmaceutical companies, and clinics. The increase in the development of smart medical equipment and mobile devices has made the healthcare industry increasingly vulnerable to ransomware, one of the most dangerous types of adaptable malware, intended to prevent entry to the system of an entity or establishment. These cybersecurity breaches consist of illegally obtaining healthcare data and ransomware events involving healthcare organizations. The healthcare industry has taken advantage of the rise of the digital revolution, resulting in unparalleled volumes of data. The healthcare industry is one of the most vital in the world, and thus, CEOs of healthcare organizations should adhere to proposed best practices to establish a strong cyberhygiene that facilitates the efficient distribution of confidential information in the face of these threats. This systematic review of the literature explores how healthcare organizations in the United States protect themselves from cyber-attack. EBook Collection (EBSCO), Google Scholar, MEDLINE, PsycINFO, PubMed, SocINDEX with Full Text, and ScienceDirect databases were sourced to answer this question. Identified themes include employee training, the need for a response plan, and strong data infrastructure.

Keywords: Cybersecurity, healthcare, leadership, ransomware, technology

Dr. William Triplett is a strategic advisor in information technology and cybersecurity with over 20 years of experience. He served as an advisor on the Cybersecurity and Information Technology Advisory Board for the Maryland Center and Bowie State University.

William continues to serve on the Chief Information Officer Council, Data Standards Council, Cybersecurity Advisory, and Technology Scientific Computing Board, and other associations to shape national-level policies and technological trends. He routinely presents at the National Institute of Standards and Technology. William has fulfilled executive-level leadership positions. He is highly sought for thought leadership on difficult open data issues and big data analytics.

William has a PhD in Strategic Leadership from Regent University, an Executive MBA from Liberty University, and a PhD in Cybersecurity Leadership from Capitol Technology University, among other degrees.

Introduction

Healthcare organizations are particularly susceptible to cyber-attacks because of the confidential data they hold which is valuable to cyber thieves (Thamer & Alubady, 2021). According to Spence et al. (2018), "Cybercriminals have begun to target the healthcare industry with ransomware, malware that encrypts an infected device and any attached devices or network drives" (p. 2). This healthcare information contains private and protected data, which can also include bank card and checking account details, classified data such as patient identification numbers, and scholastic research related to therapeutic exploration and revolution. Ransomware attacks within the healthcare setting have intensified in the past eight years (Thamer & Alubady, 2021). Many more facilities have recently suffered from the consequences of these attacks further highlighting the importance of cybersecurity.

Practitioners and information specialists are often not required to know the intricacies of ransomware attacks which can worsen the challenges they present to healthcare organizations. I argue here that the medical community must put cybersecurity first so that both patient and medical records are kept safe and confidential. While many institutions encounter cyber-attacks, the landscape of the healthcare sector presents a distinctive task as the need to prevent not only monetary damage but also patient confidentiality comes into play. Ransomware is a particularly egregious type of malware for clinics to encounter, and this potential patient data breach put healthcare organizations at security risk. Calder (2021) stated, "Someone in the UK's National Health Service clicked a link in an email. Within hours, healthcare organizations, surgeries, and offices across the country were being shut out of their own systems, causing delays to critical healthcare" (p. 7). As 2021 comes to an end, cyber-attacks have affected healthcare practices globally to how they did in 2020, with a plethora of ransomware attacks and a variety of phishing operations intended to provide hackers a grasp on the healthcare system. Ransomware ruled the world by affecting numerous corporations and healthcare operations. Healthcare facilities have become the greatest target of cyber-attacks over the past couple of years as cybercriminals continue to understand their vulnerabilities and the likelihood of these organizations to pay the ransom owed for stolen private information. Because cybercriminals are constantly changing their techniques, healthcare facilities need to continuously adopt the best defense tactics.

Problem

Healthcare practices are key targets for medical documentation theft because they lag at the tail end of other industries in terms of safeguarding crucial data. According to Burrell et al. (2021), "Despite its improvements to clinical outcomes and patient care delivery, interconnection presents unique cybersecurity vulnerabilities" (p. 21). The healthcare industry faces a substantial risk related to these attacks because it maintains so much confidential medical information. Ransomware attacks are usually carried out across multiple healthcare systems in large email phishing operations (Burrell et al., 2021). Clinics are a major focus point for these operations because they often do not upgrade their digital record-keeping systems or conduct frequent assessments to avoid modern risks and vulnerabilities (Burrell et al., 2021). This lack of precaution can majorly affect a patient's health; for example, the use of equipment that operates

on outdated computer software may not provide timely updates about patient vitals, which can lead to harmful or potentially fatal incidents (Burrell et al., 2021). Clinics also may not employ infrastructure updates to their installed equipment, leaving room for further risk. Additionally, yearly security risk evaluations that all healthcare entities are subject to are often insufficient, as there is not specific assessment methodology prescribed for these evaluations (Burrell et al., 2021). Each organization is left to design their own annual risk assessment, meaning that organizations may overlook important risk assessment activities. Clinics are again at particular risk for assessment insufficiency, as they may not employ designated IT professionals to manage their risk assessment process (Burrell et al., 2021). This vulnerability could be addressed by employing additional cybersecurity analysts to keep abreast of daily operations assignments to ensure systems are always protected from vulnerabilities. Ransomware attacks by cybercriminals have become a billion-dollar business (Calder, 2021). Data integrity is vital at all stages of healthcare confidentiality, risk insurance, and medical system safety requirements. Many physicians are unfamiliar with cybersecurity. They may also lack the necessary supplies, budget, knowledge, and infrastructure to properly prepare for cyber-attacks (Calder, 2021). Standard defense for healthcare institutions should be to apply zero trust outside institutions and to create an ever-growing collection of system security restrictions.

Consequences

Ransomware attacks on a healthcare corporation may influence other aspects of the organization besides patient information security. Mohanta et al. (2018) stated, "All kinds of ransomware can affect an organization badly" (p. 108) and expose the ways in which a firm is not prepared against an attack. Planning for malware assaults should help reduce an organization's security risks. Clinics and health systems that have been incapable of retrieving patient data caused by an attack may not be able to undertake the necessary protocols and therefore miss a significant moment in saving a patient's life (Mohanta et al., 2018).

The losses healthcare companies face from cyber-attacks can be categorized into two classifications: functional and human factors. Functional costs involve recouping money lost from ransomware attacks, which can take a substantial amount of time to recover from as every computer terminal needs to be re-examined and evaluated (Mohanta et al., 2018). Human factors focus on the correlation between individuals and information systems. People frequently forget that cybersecurity issues require an understanding of human behavior, as employees must be influenced to follow security protocols for those protocols to be effective (Corradini, 2020). The human element has historically been indicated as the most vulnerable spot in IT security, and it continues to be the weakest component in the process between the computer and the transmission of secure data (Corradini, 2020; Pollini et al., 2021). Cybersecurity focuses not only on technology, but also considers how human behavior impacts information systems. Functional costs can vary from litigation for the failure to protect confidential data or an inattention stemming from a ransomware incident. The consequences of one of these incidents can be long lasting if credibility is not quickly restored within an organization. Without up-to-date and complete access to patient medical records, errors can occur, and treatment may be inadequate. Many errors that can lead to a breach of cybersecurity are the result of employee behaviors and other

organizational factors. Individuals who experience employee burnout may forget their passwords, particularly if they are complicated (Pollini et al., 2021). Stress and long working hours can affect staff behavior and the efficiency of operations.

Impact

The healthcare industry is a key target for ransomware because of the value of patient data in organizations' custody and the profits records may produce in underground markets. In 2015, cyber-attacks cost companies $325 million worldwide, which increased to $20 billion in 2021 (Calder, 2021). Ransomware incidents continue to target larger and midsized healthcare organizations at an increasing rate (Thamer & Alubady, 2021). Criminals continue to invest time in developing spyware devices to enhance their potential manipulation of systems. Ransomware could completely shut down organization functions, which would affect patients and businesses alike. The United States healthcare organizations that were attacked in 2019 were prepared to suspend all their normal, planned scheduling and procedures until they were fully functional again (Weiner, 2021). During this time, affected patients were dispatched to other clinics in the vicinity to obtain the healthcare they needed which initiated an additional economic loss (Weiner, 2021).

Healthcare organizations are faced with the challenge of trying to protect individuals' specific information from cybercriminals. Phishing and email attacks are among the most common way cyber criminals attempt to gain access to a system (Boutwell, 2020). This happens frequently in the healthcare industry where patients have individual email accounts and may be less versed in cyber security than healthcare employees (Boutwell, 2020). However, given that the healthcare enterprise lingers at the rear of other standardized businesses in cybersecurity, workers may also not be suitably educated on how to rebuff phishing scams (Boutwell, 2020). This lack of employee understanding is critically important to healthcare companies, as the information processing systems within these institutions are by no means designed to appropriately prevent malware from email or networks within the data systems (Boutwell, 2020). The number of court disputes can also increase as a result of virus incidents because private information can be jeopardized while being cryptographed by security companies hired to prevent future attacks (Grimes, 2020). Despite this risk, information security companies still receive many requests to increase information protection from the healthcare industry.

Parenty and Domet (2019) noted, "A commonly used control to prevent phishing attacks and, more broadly, the introduction of malicious software into a corporate environment is security awareness training" (p. 13). However, healthcare organizations usually do not concentrate on cybersecurity awareness, choosing instead to focus on HIPPA conformity (Parenty & Domet, 2019). However, this leads to gaps in employee cyber awareness, and means that even new healthcare information systems are vulnerable as cyber criminals quickly evolve new techniques to breech system protections.

Attacks

Although no organization is fully protected from ransomware attacks, healthcare institutions are especially susceptible for a few reasons. Scott (2015) stated, "Healthcare organizations are required to update their legacy software periodically to stay ahead of newer security threats and avoid theft and breach of patient data" (p. 10). However, staying ahead of

attackers is becoming increasingly difficult, as computer-generated bots are becoming extremely sophisticated and can generate a swift and effortless payment for the cybercriminal (Scott, 2015). When confronted with an unparalleled cost of admission to their health archives, infrastructure systems, and information related to medical devices, healthcare organizations can feel obligated to recompense a substantial payoff to the attackers to reestablish normal processes, safeguard the security of patients, and maintain their civic image. Healthcare facilities transitioned to computerized record-keeping later than other companies, the majority of which transitioned to automated data systems between 2009 and 2015 (Parenty & Domet, 2019). In numerous examples, security tools and practices continue not to be employed, which causes delays in care services for patients. Healthcare institutions would benefit from an intervention that addresses a broad selection of technological devices. Several associated medical devices, including imagery apparatuses, embryonic screens, and intravenous monitors, are obsolete technologies that appeal to cybercriminals.

Methods

The research question this study sought to answer is: How do healthcare organizations in the United States protect themselves from cyber-attack? To answer this question a comprehensive systematic review of literature was conducted utilizing several databases. These databases included: EBook Collection (EBSCO), Google Scholar, MEDLINE, PsycINFO, PubMed, SocINDEX with Full Text, and ScienceDirect. This search included the combination of the following key words and phrases: healthcare organizations, clinics, hospitals, cyber-attack, risk reduction, and prevention. The reference list for all articles that were within inclusion criteria were individually reviewed for additional information about the literature that may not have been found in the databases.

The inclusion criteria included: 1) articles that were peer reviewed, 2) articles published in the English language, 3) articles explored how healthcare organizations in the United State protected themselves from cyber-attack 5) articles published within the last 10 years. The intent was to give the most updated research about how cyber-attack risk can be reduced among healthcare companies in the United States. Some selected articles were published prior to 2011, but they were included to provide a comprehensive view of the available research. Documents that were not published in English, non-peer reviewed articles, and literature that did not include relevant search terms were excluded.

Table 1

Articles included in this Study

Authors, Year	Purpose	Participants	Study Method	Results
Kruse et al., 2017	The objective of this systematic review is to identify cybersecurity trends, including ransomware, and identify possible solutions by querying academic literature.	31 articles	Systematic review of the literature	Healthcare should clearly define cybersecurity duties; establish clear procedures for upgrading software and handling a data breach, use VLANs and de-authentication and cloud-based computing, and to train their users not to open suspicious code.
Kamerer & McDermott, 2020	To summarizes areas of cybersecurity that directly relate to the role of the nurse as well as provide recommendations for curricular inclusion of measures to prevent or respond to a cyber-attack and mitigate the harm to patients and healthcare organizations.	26 articles	Systematic review of the literature	Implement cybersecurity curriculum for nurses in healthcare organizations using electronic health records.
Jalali et al., 2019	To identify gaps in research concerning cybersecurity response plans in healthcare.	13 articles	Systematic review of the literature	Common recommendations include construction of an incident response plan, an information security policy to act as a deterrent, and involvement of key personnel within the organization.
Nifakos et al., 2021	To identify commonly encountered factors that cybersecurity postures of a healthcare organization, resulting from the ignorance of cyber threat to healthcare.	70 articles	Systematic review of the literature	There is the need to adopt cyber hygiene practices among healthcare professionals while accessing social media platforms.
Spence, 2018	To examine recent ransomware infections in healthcare settings, the liabilities and cost associated with such infections, and discuss possible risk mitigation tactics.	29 articles	Systematic review of the literature	Results showed that if a ransomware attack is successful, healthcare providers can face substantial financial and even clinical consequences. Proper risk mitigation and disaster recovery are crucial to reduce costs and the likelihood of data loss.

Walker-Roberts et al., 2018	To ascertain the existing technological capability to mitigate insider threats within computer security systems.	18 articles	Systematic review of the literature	The effectiveness of security measures varies significantly. No solution is able to totally mitigate an insider threat.
Blanke & McGrady, 2016	To describe health care breaches of protected information, analyze the hazards and vulnerabilities of reported breach cases, and prescribe best practices of managing risk through security controls and countermeasures.	Three healthcare companies that experienced data breaches	Case study	The health care sector has the largest number of reported breaches, with 3 major types: portable device, insider, and physical breaches. Analysis of actual cases indicates security gaps requiring prescriptive fixes based on "best practices."
Coventry et al., 2020	To identify the drivers behind insecure cyber behaviors prevalent within healthcare.	50 staff at three healthcare sites	Semi-structured Interviews	Thematic analysis revealed four key facilitators of insecure behavior: Lack of awareness and experience, Shadow working processes, Behavior prioritization and Environmental appropriateness.
Argaw et al., 2020	To identify challenges cyber security experienced by hospitals and identify potential mitigating factors.	Three healthcare companies that experienced data breaches	Case study	A risk-based approach is recommended, beginning with the identification of at-risk IT assets, followed by management of tradeoffs between risks and benefits, as well as different types of risks.
He et al., 2021	To identify key cybersecurity challenges, solutions adapted by the health sector, and areas of improvement needed to counteract the recent increases in cyberattacks.	56 articles	Systematic review of the literature	Four themes were observed across the selected literature: (1) health sector condition changes due to COVID-19, (2) health care cyberattacks during the COVID-19 pandemic, (3) health care cybersecurity challenges, and (4) health care cybersecurity controls.

Results

There were several themes identified in the literature included in this study. Those themes include employee training, the need for a response plan, and strong data infrastructure.

Employee Training

Nine of the ten studies included in this review indicated that employee training was a key component of how healthcare organization in the United States protected themselves from cyber-attack. Studies contributing to this theme often indicated that employees were the weakest link in IT infrastructure, and without proper training, were likely to introduce threats into healthcare organizations' systems. For example, Spence (2018) said,

> Users have been identified as the weakest link for hackers, and user education as well as adequate detection of policy violations have the potential to make a significant difference in deterring risky end user behavior that makes a network vulnerable to attack (p. 7).

Kruse et al. (2017) reported findings very similar to Spence's (2018). Kruse et al. (2017) said,

> The most stressed security technique in the literature is proper employee training. Most security breaches are caused by employees accessing malicious files and most HIT security systems will not stop those kinds of breaches (p. 7).

To address the threat of employees allowing access to data systems, Jalai et al. (2019) recommended that, "Regardless of the size of a healthcare organization, all key personnel must be educated on the importance of information security, with an emphasis on response" (p. 83). Like Jalai et al. (2018), Kamerer and McDermott (2020) recommend healthcare organizations institute employee training. However, Kamerer and McDermott (2020) specifically recommended nurses be the recipients of this training, due to their high-level of access and contact with patient records. Kamerer and McDermott (2020) said,

> The financial and personal repercussions to patients due to breaches in PHI are significant. Healthcare organizations and employees suffer from cybersecurity threats and breaches. Because nurses play such an integral part of protecting patient PHI, healthcare technology is an integral part of their professional role. While educational programs may be one way to begin incorporating this curricular content, experienced practicing nurses may remain unaware of these important concepts related to cybercrime and cybersecurity (p. 52).

Need for a Response Plan

Five of the ten studies included in this review indicated that healthcare organizations in the United States could protect themselves from cyber-attacks by creating a strong breech response plan, and that plan should be practiced to ensure it can be implemented effectively. Argaw et al. (2020) put this plainly by saying, "As cyberattacks have become increasingly frequent and consequential in recent years, health facilities should prepare an incident response and business continuity plan" (p. 6). Blanke et al. (2017) also indicated that a response plan was critical in ensuring cyber threats could be eliminated effectively before there was a breach of sensitive patient data. However, Blanke et al. (2017)

also found that many organizations did not have such a plan:

> The digital era introduces an additional type of hazard and vulnerability to health care organizations that requires as much continuity planning as natural hazards. Yet half of the respondents in the Ponemon survey have little or no confidence that their organization has the ability to detect patient data loss or theft (p. 22).

Like Blanke et al. (2017), He et al. (2021) also found that while critical, response plans were often overlooked in organizations. He et al. (2021) recommended that organizations could reduce their risk by employing strong incident response plans. He et al. (2021) said,

> There is a lack of understanding of security risks and its impact on organization-wide risk management, such as impacts on patient care and clinical outcomes. The health sector lacks a matrix that can translate the strategic improvement needs of a health care system into prioritized information/cyber improvement needs. Schwartz et al identified that there is a lack of appreciation among health care executive management staff of the business risk impacts of cyber breaches (p. 8).

Strong Data Infrastructure

Five of the three articles reviewed in this study indicated that a strong data infrastructure was a critical way that healthcare organization in the United States protected themselves from cyber-attack. Jalai et al. (2019) indicated that part of having strong data infrastructure involved establishing effective information security policies and employing security measures to protect data. Jalai et al. (2019) said,

> There are many benefits to having a good information security policy in place. Most importantly, clearly defined security measures deter computer abuse and establish compliance. These policies need significant backing to be successful; this means support from management and the allocation of necessary funding (p. 83).

Despite the importance of a strong data infrastructure, Nifakos et al. (2021) indicated that many organizations were operating out of date systems that were not regularly updated with new and improved security features. These makeshift systems left organizations open to attack.

> However, it is noted that several healthcare organizations are muddling through cybersecurity measures, due to the size and complexity of operations, coupled with the presence of numerous legacy and stand-alone systems. This is cited as the main difficulty in implementing effective cybersecurity measures. The authors noted that the healthcare organizations have adopted the approach, 'if it ain't-broke-don't fix it' among the senior healthcare management (Nifakos et al., 2021, p. 11).

Walker-Roberts (2018) also found that having a strong data infrastructure was a key component to preventing cyber-attack. In their systematic review, Walker-Roberts (2018) posited that organizations may be looking to strengthen their data infrastructure through the use of predictive

modeling. This predictive modeling is one example of the changing landscape of data security and highlighted how implementing new technologies to ensure an up-to-date system was an important component of preventing cyber-attack. Walker-Roberts et al. (2018) stated:

> In recent years, it is apparent that there is an increasing trend within the literature towards predictive behavioral modelling to identify early malicious activity before a catastrophic data breach, though it will be clear that these behavioral systems take time to work and are therefore inappropriate in dealing with zero day or other novel inside threats.

Discussion

Liska and Gallo (2017) stated, "Ransomware is not simply a security and financial matter; it may be a reporting matter as well, depending on the regulations that govern the industry of victim organization" (p. 20). Data stored in healthcare facilities have shifted extraordinarily. The growth in technology and its transparency over the past few years has given healthcare organizations the capability to warehouse patients' data digitally. The influence of ransomware on healthcare and financial systems will remain if attacks continue to be a profitable enterprise. There is no indication from cyber thieves thus far that they are reducing their pace of attacks (Thamer & Alubady, 2021). Executing the groundwork for a cyber incident signifies readying an organization and its system to sustain it. Healthcare facilities should invest in unique, innovative, and cost-effective products that will assist in defending their systems from malware. An example of this is Walker-Roberts' (2018) finding that predictive modeling is becoming increasingly important in the data security landscape for healthcare organizations. However, despite some promising improvements, gaps in cybersecurity remain. According to Parenty and Domet (2019), "Many directors have told us that cybersecurity is daunting, if not overwhelming. They feel as if they're making investment decisions without reliable data and don't fully understand the capabilities of cybersecurity technologies" (p. 30). Recovering from a data breach requires a substantial amount of time and skill to ensure that systems are operating accurately and successfully again. This finding of the literature is supported by the findings of this study, which include that the establishment of strong response plans is critical to preventing data loss due to cyber-attack.

Another finding of this study was that employee training was an important component in preventing cyber-attack. A prerequisite is the employee, needs to practice in real-time. This practice should be combined with security professionals who conduct assessments and testing in big groups given the size of the organization can support large groups. Pettit (2017) stated, "Ransomware can encrypt computer files until a ransom is paid to unlock them and may include not only the encryption of user-generated data files but may include server or workstation operating system files such that the server or computer is rendered non-functional" (p. 10). Though institutions consider their options before a decision is made, to prevent further destruction from ransomware, some businesses may choose to pay the ransom outright. This further feeds the business of cybercrime and encourages attacks to continue.

Recommendations

Healthcare administrations must offer cybersecurity education to the same degree

that they offer education about the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Scott (2015) indicated, "Digital healthcare data such as PHI must be protected, since health information often has to be shared externally with providers, insurers and other third parties who, in turn, can forward it to other parties" (p. 4). Consequently, cybersecurity ought to be considered as important as HIPAA since without proper security measures, patient confidentially may be breeched in addition to the exposure of financial information. Executives ought to provide necessary training to teach the medical workforce about cybersecurity vulnerabilities to ensure that teams are prepared for cyber-attacks. Further, health organizations must recognize the value of acquiring the essential expertise needed to identify these cyber incidents and know the steps to take to prevent and report the attacks. Healthcare executives must highlight the significance of cybersecurity awareness to employees with the goal of diminishing the loss suffered when patient data is compromised. The cyber industry changes constantly, and thus healthcare financial statements must continuously adapt and have the capacity to change swiftly and effectively (Thamer & Alubady, 2021). For organizations to prepare for these complications, their cybersecurity plans must be sufficient to deliver all required training. Ransomware has affected countless businesses and healthcare facilities. The executive team must be completely engaged in the development and implementation of these training obligations. There must be a total organizational commitment to training employees and implementing appropriate system defenses for these attacks otherwise the organization will not be able to mount a successful defense.

References

Argaw, S. T., Troncoso-Pastoriza, J. R., Lacey, D., Florin, M.-V., Calcavecchia, F., Anderson, D., Burleson, W., Vogel, J.-M., O'Leary, C., Eshaya-Chauvin, B., & Flahault, A. (2020). Cybersecurity of Hospitals: Discussing the challenges and working towards mitigating the risks. BMC Medical Informatics and Decision Making, 20(1), 146. https://doi.org/10.1186/s12911-020-01161-7

Blanke, S. J., & McGrady, E. (2016). When it comes to securing patient health information from breaches, your best medicine is a dose of prevention: A cybersecurity risk assessment checklist. Journal of Healthcare Risk Management, 36(1), 14–24. https://doi.org/10.1002/jhrm.21230

Boutwell, M. (2020). The ransomware handbook: How to prepare for, prevent, and recover from ransomware attacks. Pallas Group.

Burrell, D. N., Aridi, A. S., McLester, Q., Shufutinsky, A., Nobles, C., Dawson, M., & Muller, S. R. (2021). Exploring system thinking leadership approaches to the healthcare cybersecurity environment. International Journal of Extreme Automation and Connectivity in Healthcare (IJEACH), 3(2), 20–32.

Calder, A. (2021). The ransomware threat landscape: Prepare for, recognise and survive ransomware attacks. IT Governance. ISBN: 1787782786, 9781787782785

Corradini, R. (2020). Building a cybersecurity culture in organizations: How to bridge the gap between people and digital technology. Springer Nature.

Grimes, A. (2022). Ransomware protection playbook. John Wiley & Son, Inc.

He, Y., Aliyu, A., Evans, M., & Luo, C. (2021). Health Care Cybersecurity Challenges and Solutions Under the Climate of COVID-19: Scoping Review. Journal of Medical Internet Research, 23(4), e21747. https://doi.org/10.2196/21747

Jalali, M. S., Russell, B., Razak, S., & Gordon, W. J. (2019). EARS to cyber incidents in health care. Journal of the American Medical Informatics Association, 26(1), 81–90. https://doi.org/10.1093/jamia/ocy148

Kamerer, J. L., & McDermott, D. (2020). Cybersecurity: Nurses on the Front Line of Prevention and Education. Journal of Nursing Regulation, 10(4), 48–53. https://doi.org/10.1016/S2155-8256(20)30014-4

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, 25(1), 1–10. https://doi.org/10.3233/THC-161263

Liska, A., & Gallo, T. (2017). Ransomware: Defending against digital extortion. O'Reilly Media, Inc.

Moallem, A. (Ed.). (2020). HCI for cybersecurity, privacy and trust: Second international conference, HCI-CPT 2020, held as part of the 22nd HCI international conference, HCII 2020, Copenhagen, Denmark, July 19-24, 2020: proceedings. Springer.

Mohanta, A., Hahad, M., & Velmurugan, K. (2018). Preventing ransomware: Understand, prevent, and remediate ransomware attacks. Packt Publishing.

Nifakos, S., Chandramouli, K., Nikolaou, C. K., Papachristou, P., Koch, S., Panaousis, E., & Bonacina, S. (2021). Influence of Human Factors on Cyber Security within Healthcare Organisations: A Systematic Review. Sensors, 21(15), 5119. https://doi.org/10.3390/s21155119

Parenty, D. J., & Domet, J. (2019). A leader's guide to cybersecurity: Why boards need to lead—and how to do it. Harvard Business Review Press.

Pettit, T. (2017). Ransomware: Prevention and recovery: How to avoid paying a ransom. CreateSpace Independent Publishing.

Pollini, A., Callari, T. C., Tedeschi, Ruscio, A. D., Save, L., Chiarugi, F., & Guerri, D. (2021). Leveraging human factors in cybersecurity: An integrated methodological approach. Cognition, Tech & Work. https://doi.org/10.1007/s10111-021-00683-y

Scott, J. (2015). Cybersecurity hygiene for the healthcare industry: The basics in healthcare IT, health informatics and cybersecurity for the healthcare sector (Vol. 4).

Spence, N., Niharika Bhardwaj, M. B. B. S., & Paul, D. P. III (2018). Ransomware in healthcare facilities: A harbinger of the future? Perspectives in Health Information Management, Summer, 1–22. https://perspectives.ahima.org/wp-content/uploads/2018/06/RansomwareinHealthcare.pdf

Spence, N., Paul, III, D. P., Bhardwa, N., Coustasse, A. (2018, April). Healthcare Facilities: Another Target for Ransomware Attacks. Presented at the 54th Annual MBAA Conference, Chicago, IL.

Thamer, N., & Alubady, R. (2021). A survey of randsomeware attacks for healthcare systems: Risks, challenges, solutions and opportunity of research. 1st Babylon International Conference on Information Technology and Science (2021, August 12). http://doi.org/10.1109/BICITS51482.2021.9509877

Walker-Roberts, S., Hammoudeh, M., & Dehghantanha, A. (2018). A Systematic Review of the Availability and Efficacy of Countermeasures to Internal Threats in Healthcare Critical Infrastructure. IEEE Access, 6, 25167–25177. https://doi.org/10.1109/ACCESS.2018.2817560