INSTITUTE FOR HOMELAND SECURITY

Sam Houston State University

MITIGATING CYBERSECURITY THREATS TO HOSPITALS AND HEALTHCARE FACILITIES

Institute for Homeland Security

Sam Houston State University

Peter S. Lehmann, Ph.D.

Alexander B. Kinney, Ph.D.

Mitigating Cybersecurity Threats to Hospitals and Healthcare Facilities

Peter S. Lehmann, Ph.D. https://orcid.org/0000-0002-5345-4343 Alexander B. Kinney, Ph.D. https://orcid.org/0000-0003-2916-1791

Abstract

Healthcare facilities rely heavily on digital information systems to deliver patient care and manage confidential patient information. However, healthcare networks and medical devices are highly vulnerable to attackers, who can use the information to victimize medical facilities as well as the patients themselves. The functioning of healthcare systems can be seriously impeded by cyberattacks, restricting information sharing among hospital personnel and delaying or preventing patient care. Although federal legislation and regulatory guidelines have been put forth to improve responses to cyberattacks and enhance patient information protections, the cybersecurity measures in place in many hospitals can be easily bypassed by motivated offenders via entry points in the facilities' cybersecurity systems. In response to these threats to critical infrastructure, experts have proposed several risk mitigation strategies that healthcare facilities can employ to improve information technology systems and mitigate vulnerabilities associated with human factors. This report provides a summary of (1) the literature on the types and characteristics of cyberattacks most often perpetrated against healthcare providers, (2) the theory and research from criminology and criminal justice on the factors associated with cybercrime victimization risk, and (3) the best practices proposed by experts to help inform policymakers and healthcare professionals in Texas and nationwide.

Keywords: cybersecurity, healthcare, cybervictimization, medical technology, patient information

Introduction

As the modern healthcare field has become increasingly dependent on technology, responses to cybersecurity threats and the prevention of cyberattacks have emerged as a top priority for hospitals and healthcare facilities (Martin et al., 2017; Tully et al., 2020). One estimate from 2014 revealed that 94% of healthcare institutions had been the victim of a cyberattack (Perakslis, 2014), and recent evidence suggests that the frequency of healthcare data breaches has more than tripled in the past decade (Wasserman & Wasserman, 2022). Further, the COVID-19 pandemic led to a sharp rise in cybervictimization against hospitals, as heightened staff workload, the implementation of new forms of software, and loosened safeguards over datasharing practices rendered these sites particularly vulnerable (Muthuppalaniappan et al., 2021; Saleous et al., 2023; Williams et al., 2020). The healthcare industry is more commonly targeted by cyberattacks than the financial sector, with healthcare facilities representing the victims of 24% of all cyberattacks (Argaw et al., 2020).

The healthcare field is affected by several forms of cyberthreats, with financial gain on the part of the perpetrator being the intended outcome in most instances. For instance, malicious software may be introduced to networks whereby patient records and other secure data are accessed and encrypted (i.e., "cryptographic attacks"), with hackers threatening to expose or sell the data if a ransom is not paid (Argaw et al., 2020; Slayton, 2018; Spence et al., 2018). Data breaches also can occur through "eavesdropping" (i.e., "Man-in-the-Middle" attacks) on private communications, "privilege escalation" by means of converting a regular login account to one with administrative credentials, phishing attacks via mass emails and/or emails targeted to specific individuals, and the physical insertion of infected hardware (e.g., USBs, external hard drives, or compact disks) into secure computers (Bhuyan et al., 2020; Wasserman & Wasserman,

2022). Successful healthcare data breaches can be very lucrative for perpetrators, as compliance with ransom demands often is less costly for hospitals than the loss of revenue resulting from a network shutdown (Williams et al., 2020).

Other individuals and groups may perpetrate cyberattacks to achieve political ends (e.g., "hacktivists"), to express resentment toward a particular healthcare facility or physician, for the personal enjoyment of the perpetrator(s), or by non-malicious "white hat" actors to discover vulnerabilities so they can be addressed (Beavers et al., 2019; Bhuyan et al., 2020; Wilner et al., 2019). Rather than exploit vulnerable networks for financial incentives, some of these attacks are intentionally destructive. For instance, denial-of-service (DoS) attacks overwhelm network traffic in order to compromise a hospital's reputation and/or physically harm patients (Langer, 2017). Certain forms of malware are designed not to steal, modify, or encrypt confidential patient information but rather to simply destroy files. A related form of cyberattack is the "spoofing" of medical devices to steal data, adjust their settings, manipulate information, or render them inoperable for purposes of causing injury (Ayala, 2016; Sethuraman et al., 2020; Wasserman & Wasserman, 2022).

Problem Statement and Research Objective

Reducing vulnerabilities to cyberattacks represents a key concern among healthcare professionals nationwide, and several recent and highly publicized incidents in Texas have highlighted the relevance of these issues in the state (e.g., Collier, 2022; Gill, 2022; Miles, 2022; Starks & DiMolfetta, 2023; Tilley, 2022). The scope and frequency of these attacks present serious threats to the quality of patient care (Jalali & Kaiser, 2018; Jarrett, 2017; Tully et al., 2020) as well as the protection of patients' private information that, if leaked, could render them susceptible to identity theft and medical fraud (Argaw et al., 2020; Gordon et al., 2017). The

interconnected nature of information-sharing within and across hospital networks, the unique vulnerabilities of healthcare devices, the ineffective infrastructure in place in many healthcare facilities, and the lack of knowledge and proper training among personnel represent some key areas in which improvements may be made to enhance healthcare facilities' cybersecurity protection and help them more effectively prevent and respond to threats (Abraham et al., 2019; Ahmed et al., 2022; Middaugh, 2021).

The aim of this report is threefold. First, through a review of the relevant literature on cybersecurity, hospital information management, and healthcare systems and technology, we provide a summary of the types and characteristics of cyberattacks commonly perpetrated against hospitals and healthcare providers in Texas and across the country, emphasizing in particular the costs and consequences associated with these incidents. Second, in light of the vast body of research from criminology and criminal justice identifying the risk and protective factors which increase and decrease the likelihood of cybercrime victimization generally, we briefly review these relevant theoretical and empirical developments in order to gain insights that may be applied to healthcare facilities' experiences with cyberthreats. Finally, we use this literature to develop a set of effective cybersecurity practices that hospitals and medical facilities may implement to better respond to and protect against cyberattacks.

Characteristics of Cyberattacks Against Healthcare Facilities

Cyberattacks on health technology and networks require a point of entry. Upon gaining access, the perpetrators assess the type and value of the data available and identify the ways in which any vulnerabilities with the system or device may be exploited. Then, the malicious party targets the system by stealing the valuable information or modifying, hindering, or shutting down its operation (Langer, 2017; Martignani, 2019). Cyberattacks may be passive or active; passive

attacks involve stealing confidential information (e.g., patient records) whereas active attacks require the interception, adjustment, or destruction of a system's functions or a medical device's operations (Wasserman & Wasserman, 2022). While motivated perpetrators often deliberately target specific facilities or institutions, the attacks themselves frequently are opportunistic in nature (Luna et al., 2016), and the specific strategies employed after gaining access to a vulnerable system vary according to the offenders' desired outcome. Understanding the types of cyberattacks—and what goals each may accomplish—is essential for transforming cybersecurity responses from reactive to proactive (Bhuyan et al., 2020).

Types of Cyberattacks

A common and potentially lucrative form of cyberattack against healthcare facilities is the introduction of ransomware via a "cryptographic attack" (Bhuyan et al., 2020; Dameff et al., 2023). A typical ransomware attack involves hacking a facility's record-keeping system and reencrypting the data to block access by hospital staff until ransom demands are met (Farringer, 2016; Neprash et al., 2022; Spence et al., 2018). This type of attack was experienced by several major healthcare systems in Texas, including Methodist Health System (Miles, 2022), St. Luke's Health (Gill, 2022), and OakBend Medical Center (Tilley, 2022). The extortion of hospitals can reap large monetary benefits, as hospitals are frequently incentivized to pay the ransom:

> [T]he University of California, San Francisco (UCSF) was hacked by the cybercrime group "Netwalker," who demanded payment in exchange for not releasing confidential information. Out of fear of the consequences of this information's release, UCSF paid the group US $1.14 million. The same group also took over the Champaign Urbana Public Health District website. Similarly, the Hollywood Presbyterian Medical Center in Los Angeles paid US $17,000 to get a decryption key to regain access to their hospital system. Although they regained access, they lost 10 days of revenue and likely took a hit to their reputation. Unfortunately, however, complying with the demands of the cybercriminal may in fact be the most cost-effective solution, as a successful cyberattack costs an average of US $3.7 million to recover from. Additionally, failure to comply can pose a serious threat to patient safety. (Williams et al., 2020, p. 2)

Even when hospitals do not comply with ransom demands, electronic health records (EHRs) are highly valuable in darknet markets (Martin et al., 2017). Accordingly, a variety of mechanisms can be used to infiltrate hospital systems and gain access to patient records even if no cryptographic attack occurs. Phishing scams involve tricking legitimate users of restricted data (e.g., hospital staff) via a seemingly legitimate email or link, often sent to a large number of people (Yeo & Banfield, 2022). These attacks are highly successful, even under highly secure systems (Healthcare Information and Management Systems Society, 2020), and one simulation study showed that one in seven healthcare employees (i.e., 14.2%) clicked on infected email links (Gordon et al., 2017). To further increase the effectiveness of this strategy, attackers can send personalized, targeted emails to select users (i.e., "spear phishing"), especially individuals in positions of authority (i.e., "whale phishing"). One reason that phishing is so effective is that the deception is disguised through social engineering, as the messages appear to originate from peers, IT staff, or other reliable sources (Priestman et al., 2019).

Malicious software (e.g., viruses, worms, trojans, etc.) also can be introduced through corrupted external hardware that is connected to hospital equipment by unaware healthcare personnel (Bhuyan et al., 2020). As one study explains:

> Physical insertion of malware can be just as potent as phishing. Frequently mentioned in the literature are attacks in which infected USBs, external hard drives, or compact disks are "accidentally" left in employee parking lots. The expectation is that well-meaning staff members who find the devices will plug them into hospital computers to check the files and identify the devices' owners. Indeed, in an experiment by the U.S. Department of Homeland Security, sixty percent of its employees who found devices in the parking lot inserted those devices into government computers. This number was higher, 90%, if the device carried a government or contractor logo. (Wasserman & Wasserman, 2022, p. 5)

Another method of accessing restricted data is "eavesdropping," also known as a Man-in-theMiddle (MitM) attack, which involves a reconnaissance strategy whereby an attacker intercepts communication between two parties and steals data, modifies the data, or secretly attaches malware to those communications (Ayala, 2016; Nifakos et al., 2021). Malicious software also can be introduced to healthcare networks through privilege escalation of login credentials, which are frequently accessed via phishing (Langer, 2017). Indeed, it is not uncommon for several of these attack strategies to be employed in concert.

Some cyberattacks do not involve the exploitation of networks and individuals to steal valuable patient data but rather are deployed to cause destruction. These tactics are often perpetrated by threat groups to send political messages, by patients to express anger toward a specific hospital or physician, by former employees to exact revenge, or by anonymous actors for personal amusement (Luna et al., 2016; Wasserman & Wasserman, 2022). Denial-of-services (DoS) represent a large proportion of these attacks; through this strategy, actors flood a network with traffic to such an extent that patient data cannot be sent or received, and the network becomes inaccessible. Additionally, certain forms of malware have been deployed by militaries against a wide range of high-value infrastructure targets to destabilize power grids and shut down hospitals, airports, government offices, and financial institutions (Pullin, 2018). Specific portable healthcare devices also can be "spoofed" via their acoustic frequencies to adjust their settings (Sethuraman et al., 2020), manipulate diagnostic images (Eichelberg et al., 2020, 2021), or cease their operation with the goal of causing harm to patients.

Costs and Consequences of Cyberattacks

The financial and human costs associated with cyberattacks are wide-ranging, varying according to the type and scope of the attack, the specific target, and the ability of the system to

respond effectively to mitigate damage. In addition to ransom payments, equipment repair, and legal fees, hospitals must manage an extensive list of other associated financial costs: public relations costs, credit protection services for affected patients, loss of revenue due to medical appointments canceled by necessity or patient request, investments in the employment and training of cybersecurity personnel, and increased insurance premiums (Healthcare Information and Management Systems Society, 2020; Peterson et al., 2018; Wasserman & Wasserman, 2022). Further, the Health Insurance Portability and Accountability Act (HIPAA) of 1996 and the subsequent Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 impose substantial fines on healthcare systems for violations of patient information protection regulations (Argaw et al., 2020; Cohen & Mello, 2018). In total, the financial costs of data breaches can be immense, and some recent large-scale attacks have cost hospital systems tens of millions or hundreds of millions of dollars (Tully et al., 2020).

The public health costs associated with cyberattacks can be difficult to measure. Indeed, though the specific outcomes depend on the focus of the cyberattack, patient care can be affected in myriad ways by these events. As Argaw and colleagues (2020) illustrate:

> Cyberattacks can threaten a wide variety of services within a hospital, from surgeries to drug delivery, by targeting advanced equipment such as blood-product refrigerators, imaging equipment, automated drug dispensers and electronic health records, as well as by targeting supporting critical systems such as heating, ventilation, and air conditioning (HVAC). When EHR integrity is compromised, or they are suddenly encrypted in an attack, such as ransomware, providers lose access to critical information (e.g., patient allergies, current medications, and comorbidities). Hospitals are especially at risk in extreme or conflict situations, where stealth malware can stay hidden in the system until conveniently activated, thus leading to severe consequences when healthcare is most urgent (e.g., following a natural or human-instigated disaster). (p. 2)

In the event of a cyberattack on the facility's network, hospital staff may be unable to use certain medical devices, transport patients and lab samples via elevators, or run systems that help keep

operating rooms sterile (Argaw et al., 2020; Ayala, 2016). Notably, inaccess to patient health records, medication information, and diagnostic images can delay patient care and/or cause staff to administer incorrect medication dosages (Eichelberg et al., 2020). The remote manipulation of medical devices can cause serious patient injury; for instance, an attack that triggers a dose reduction in an insulin pump can induce hyperglycemia, diabetic ketoacidosis, or death (Alexander et al., 2019; Wasserman & Wasserman, 2022). Vulnerable devices may need to be replaced, which can require invasive surgery. More broadly, responses to disruptions to patient care often require diverting resources to unaffected systems, thus making the extent of the human costs of these cyberattacks particularly far-reaching (Dameff et al., 2023).

The consequences of specific cyberattacks are not always made known to the public in news media reports. However, the numbers of confidential patient records that were stolen in successful attacks are sometimes publicly available. For instance, the recent cyberattack on St. Luke's Health affected nearly 17,000 patients (Fox, 2022), and the OakBend Medical Center ransomware attack in October 2022 rendered more than 500,000 patients' information vulnerable to identity theft (Tilley, 2022). These and other cyberattacks in Texas also caused patient carerelated issues, such as delays due to a transition to paper charting, an inability to complete lab work, canceled appointments, and postponed surgeries (Chow & Ford, 2022; Collier, 2023; Gill, 2022). The long-term effects of these individual events are not yet known, though research on national and international trends indicates that hospitals that are the victims of data breaches also experience subsequent increases in patient mortality rates (Choi et al., 2019; Tully et al., 2020;

Wasserman & Wasserman, 2022).

Theory and Research on Cybercrime Victimization

Empirical attention in the field of criminology and criminal justice has long been devoted to the predictors and consequences of offending and victimization, but only recently has focus turned to cybercrime. Much of the research in this area examines the cybervictimization of individuals, emphasizing the financial losses and detriments to well-being and lifestyle that result from hacking, identity theft, and other personal data breaches (e.g., Feinstein et al., 2014; Gardella et al., 2017; Turanovic & Pratt, 2019). Though individual-level correlates of cybervictimization include such factors as low sensitivity to risk (Bossler & Holt, 2010; Louderback & Antonaccio, 2021; Partin et al., 2022; Reyns et al., 2019) and participation in certain high-risk online activities (Bossler et al., 2012; Choi & Lee, 2017; Ngo & Paternoster, 2011), this literature also suggests that prevention efforts can effectively reduce victimization risk. Accordingly, this body of work may provide insights into the risk and prevention factors that are associated with the cybervictimization of healthcare facilities, not least since human factors are the source of many hospital cybersecurity breaches (Middaugh, 2021; Yeng et al.,
2022; Yeo & Banfield, 2022).

The Routine Activities Framework

Routine activities theory posits that victimization events occur when several factors converge in time and space: a motivated offender, a suitable target, and the absence of capable guardianship (Cohen & Felson, 1979). In online spaces, the temporal aspect of crime events is complicated, as even when stable network connections make victimization—including highly targeted victimization—a constant threat (see, e.g., Brady et al., 2016; Yar, 2005), access to the points of entry that permit cyberattacks are frequently opportunistic (Lallie et al., 2021; Lee & Wang, 2022; Minnaar & Herbig, 2021). In the context of cybervictimization at the individual

level, engaging in risky online behaviors, especially those which involve sharing one's personal information, can render a target more suitable (Choi & Lee, 2017; Reyns, 2013). Thus, as inhibiting offender motivation is rarely feasible for potential victims, the most effective crime prevention solutions, including efforts intended to reduce the likelihood of cybervictimization, hinge on reducing target suitability and improving guardianship.

Recent research in criminology and criminal justice has applied the routine activities framework to understand variation in individuals' risk of cybervictimization (Holt & Bossler, 2008; Leukfeldt & Yar, 2016; Pratt et al., 2010). This research reveals that willful involvement in high-risk online activities is a strong predictor of cybercrime victimization (e.g., Choi & Lee, 2017; Ngo et al., 2020; Partin et al., 2022), but neglectful behavior and an ignorance of one's own vulnerability to attack are salient factors as well (Henson et al., 2013; Lee & Wang, 2022; Reisig et al., 2009). Indeed, users of wireless networks, email systems, and computer devices are frequently unaware of the ways in which these technologies may be exploited and how their own behavior can facilitate a cyberattack. Accordingly, even individuals who regularly use otherwise vulnerable technology often can mitigate their suitability as targets for victimization through the employment of mindful best practices. Further, capable guardianship against cyberthreats can be heightened through the use of protective software and equipment that is regularly updated (Holt & Bossler, 2008; Ngo & Paternoster, 2011).

Relevance of Routine Activities for Healthcare Cybersecurity

Healthcare facilities are not equipped to address the financial, political, or personal motivations that drive cybercrime perpetration. However, as 40% of cyberattacks are induced through actions of unaware staff members (Healthcare Information and Management Systems Society, 2020), human error and failure to adhere to accepted cyber-hygiene protocols and

practices represent a key source of target suitability that makes cyberattacks more likely (Swede et al., 2019; Wasserman & Wasserman, 2022). Several unique features of the healthcare field amplify these "human factor" issues, including the intense focus on patient care, the lack of time and resources available for adequate cybersecurity measures, and high personnel turnover that necessitates the frequent retraining of newly hired staff (Gordon et al., 2017; Nifakos et al., 2021). Thus, even a strong cybersecurity infrastructure is likely to be subject to attacks if end users act in ways that unknowingly render its systems vulnerable (Kruse et al., 2017). Yeng et al. (2022) explain this issue thusly:

> [I]nformation security solutions have traditionally been focused on technical measures such as firewall configurations, demilitarize zone, intrusion detection and prevention systems, authentication, and authorizations in mitigating risks; however, the human aspect of IS management (also called the human firewall) has received less attention as an important factor in mitigating security issues. Meanwhile, current dynamics in security issues cannot be resolved with only technical measures especially in an era where humans are considered the weakest link in the security chain. (p. 1)

Thus, as in the mitigation of individual victimization risk in online and offline settings, decisions made without careful consideration of the associated potential risks can make targets more attractive to motivated perpetrators (Coventry & Branley, 2018).

Notwithstanding the importance of human factors, capable guardianship remains a key facet of cybervictimization prevention at the personal (Milani et al., 2022; Ngo & Paternoster, 2011) and institutional levels (Buil-Gil et al., 2021). In a healthcare setting, hospitals with inadequate cybersecurity infrastructures are at risk of data breaches and other cyberattacks, and the notable disparities in security controls between the healthcare and financial sectors may explain why cyberattacks against the financial industry are far less common (Choi & Johnson, 2021). One distinct vulnerability in this regard is that hospitals are moving away from intranet systems to house patient records and instead are using cloud-based data storage, which is cheaper

and easier for file-sharing but is far more vulnerable to external threats (Wasserman & Wasserman, 2022). Additionally, picture archiving and communication systems (PACS), which are increasingly relied upon for diagnostic purposes by radiologists in lieu of physical images, are often similarly vulnerable (Eichelberg et al., 2020, 2021). Relatedly, security systems on medical devices that allow for continuous monitoring and treatment of both inpatients and outpatients are often weak, out-of-date, and easily bypassed even by amateurs (Sethuraman et al., 2020; Tomaiko et al., 2021).

Promoting Effective Cybersecurity Responses

Technological advances in the healthcare field have enhanced patient care and datasharing within and across hospital systems, though these developments have been attended by notable cybersecurity risks. Indeed, not only must risk mitigation and prevention efforts involve securing medical devices and networks but they also should address the various human factors through which the behavior of unwitting staff members can render systems vulnerable to cyberattacks. Further, commenters have noted that regulatory measures and guidelines in place which are intended to inform cybersecurity responses can be inconsistent and impractical. Accordingly, below is a summary of some of the recommendations for policy and practice that experts have proposed to address these various issues and concerns. These responses relate to (1) securing vulnerable infrastructure and devices, (2) addressing staff behavior through training, and (3) improving consistency in the guidelines provided by regulatory bodies.

Securing Infrastructure

Healthcare facilities should implement procedures that require the consistent monitoring and assessment of IT vulnerabilities, as early detection of cybersecurity risks is essential to mounting an effective response (Bhuyan et al., 2020). Though not always successfully

preventative (Wasserman & Wasserman, 2022), the proper maintenance and patching of a system's IT infrastructure—including third-party software—is a central component of this process. As Argaw et al. (2020) explain:

> [C]onfiguration management has the benefit of increasing ease in assessing vulnerabilities because of a broader understanding of the facilities' IT infrastructure and in running risk assessments, as well as analyses required for patch processes. Patching should be applied to all systems in the configuration (this includes the operating system and third-party applications) and changes should be noted by change management. (pp. 56)

Additionally, sensitive information can be better protected through the implementation of various software-based approaches, including "segmenting" a network into small sections that can be isolated in the event of an attack, limiting the number of staff members who have administrative privileges within networks, restricting the types of online activity that can occur from accounts logged in with administrator credentials, and immediately revoking employees' account access when no longer in use (Argaw et al., 2020; Sittig & Singh, 2016). Other similar measures can involve mandating regular password updates, implementing automatic file-backup systems, restricting network access only to approved devices, blocking access to certain websites, and using antivirus and antimalware programs (Wasserman & Wasserman, 2022).

Training and Staff Responses

For the reasons previously discussed, healthcare facilities frequently provide inadequate cybersecurity training for their employees (Gordon et al., 2017; Nifakos et al., 2021). However, the human factors associated with cyberthreat mitigation have been emphasized in much prior work in this area, and addressing these gaps through training is essential (Bhuyan et al., 2020). A key dimension of cybersecurity training is the development of an incident response plan:

> As cyberattacks have become increasingly frequent and consequential in recent years, health facilities should prepare an incident response and business continuity plan. These

> plans should be regularly tested, exercised, and stored offline. Plans should involve an agreed upon process with the appropriate stakeholders identified. It is important to have a designated team and a cybersecurity leader, or simply a designated person in cases where the organization does not have a CISO. The roles and responsibilities should be clearly divided within the team. The organizations should also have an agreement on what constitutes as a reportable incident and when to escalate. Ideally, plans should embed prevention training as well. (Argaw et al., 2020, p. 6).

Inadequate preparedness for cyberattacks became particularly apparent during the COVID-19 pandemic, not least because staff members were unaware of the risks associated with the use of certain third-party platforms used for telemedicine, the vulnerabilities associated with their own personal devices, and the effects of stress on their decision-making (Muthuppalaniappan et al., 2021; Saleous et al., 2023; Williams et al., 2020). As social engineering tactics constantly evolve, employees should be regularly informed of best practices, and cybersecurity education should become enculturated within healthcare facilities (Georgiadou et al., 2021).

Regulatory Guidelines

Finally, although federal law requires hospitals to have information security protocols in place to protect confidential patient information (Jalali & Kaiser, 2018; Perakslis, 2014), simple adherence to these basic policy regulations is likely to be insufficient. However, the guidelines provided by the various regulatory agencies can be convoluted and contradictory, and there is little consensus about which specific set of guidelines should be followed (Wasserman & Wasserman, 2022). Moreover, small facilities may not be adequately situated to implement the preventative measures recommended by these agencies, leaving them to develop their own cybersecurity systems that frequently are vulnerable to attack. The healthcare field should address this incongruence surrounding cybersecurity best practices and mixed adherence to best practice guidelines, though the development of a more unified approach should be sensitive to the realities regarding differences in hospitals' operations, deficiencies in staff training, and a

lack of resources available for cyberthreat prevention and mitigation in many facilities. Nonetheless, improving the consistency and uniformity of cybersecurity guidelines likely would be beneficial for guiding hospitals' cybersecurity planning and implementation.

References

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, M. A., Sindi, H. F., & Nour, M. (2022). Cybersecurity in hospitals: An evaluation model. *Journal of Cybersecurity and Privacy*, *2*(4), 853-861. https://doi.org/10.3390/jcp2040043

Alexander, B., Haseeb, S., & Baranchuk, A. (2019). Are implanted electronic devices hackable? *Trends in Cardiovascular Medicine*, *29*(8), 476-480. https://doi.org/10.1016/j.tcm.2018.11.011

Argaw, S. T., Troncoso-Pastoriza, J. R., Lacey, D., Florin, M. V., Calcavecchia, F., Anderson, D., ... & Flahault, A. (2020). Cybersecurity of hospitals: Discussing the challenges and working towards mitigating the risks. *BMC Medical Informatics and Decision Making*, *20*, Article 146. https://doi.org/10.1186/s12911-020-01161-7

Ayala, L. (2016). *Cybersecurity for hospitals and healthcare facilities: A guide to detection and prevention*. Springer. https://doi.org/10.1007/978-1-4842-2155-6

Beavers, J., Pournouri, S. (2019). Recent cyber attacks and vulnerabilities in medical devices and healthcare institutions. In H. Jahankhani, S. Kendzierskyj, A. Jamal, G. Epiphaniou, & H. Al-Khateeb (Eds.), *Blockchain and clinical trial: Advanced sciences and technologies for security applications* (pp. 249-267). Springer. https://doi.org/10.1007/978-3-030-112899_11

Bhuyan, S. S., Kabir, U. Y., Escareno, J. M., Ector, K., Palakodeti, S., Wyant, D., ... & Dobalian, A. (2020). Transforming healthcare cybersecurity from reactive to proactive: Current status and future recommendations. *Journal of Medical Systems*, *44*, 1-9. https://doi.org/10.1007/s10916-019-1507-y

Bossler, A. M., & Holt, T. J. (2010). The effect of self-control on victimization in the cyberworld. *Journal of Criminal Justice*, *38*(3), 227-236. https://doi.org/10.1016/j.jcrimjus.2010.03.001

Bossler, A. M., Holt, T. J., & May, D. C. (2012). Predicting online harassment victimization among a juvenile population. *Youth & Society*, *44*(4), 500-523. https://doi.org/10.1177/0044118X11407525

Brady, P. Q., Randa, R., & Reyns, B. W. (2016). From WWII to the World Wide Web: A research note on social changes, online "places," and a new online activity ratio for routine activity theory. *Journal of Contemporary Criminal Justice*, *32*(2), 129-147. https://doi.org/10.1177/1043986215621377

Buil-Gil, D., Lord, N., & Barrett, E. (2021). The dynamics of business, cybersecurity and cybervictimization: Foregrounding the internal guardian in prevention. *Victims & Offenders*, *16*(3), 286-315. https://doi.org/10.1080/15564886.2020.1814468

Choi, K. S., & Lee, J. R. (2017). Theoretical analysis of cyber-interpersonal violence victimization and offending using cyber-routine activities theory. *Computers in Human Behavior*, *73*, 394-402. https://doi.org/10.1016/j.chb.2017.03.061

Choi, S. J., & Johnson, M. E. (2021). The relationship between cybersecurity ratings and the risk of hospital data breaches. *Journal of the American Medical Informatics Association*, *28*(10), 2085-2092. https://doi.org/10.1093/jamia/ocab142

Choi, S. J., Johnson, M. E., & Lehmann, C. U. (2019). Data breach remediation efforts and their implications for hospital quality. *Health Services Research*, *54*(5), 971-980. https://doi.org/10.1111/1475-6773.13203

Chow, S., & Ford, B. (2022). 'Ransomware attack': St. Luke's Health working to restore functionality, systems. *KHOU 11*. https://www.khou.com/article/news/local/st-lukeshealth-commonspirit-ransomware-attack/285-2c56adce-5d96-472c-9cab-40b9a4cbb4bc

Cohen, I. G., & Mello, M. M. (2018). HIPAA and protecting health information in the 21st century. *JAMA*, *320*(3), 231-232. https://doi.org/10.1001/jama.2018.5630

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

Collier, K. (2022, October 7). Ransomware attack delays patient care at hospitals across the U.S. *NBC News*. https://www.nbcnews.com/tech/security/ransomware-attack-delays-patientcare-hospitals-us-rcna50919

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

Dameff, C., Tully, J., Chan, T. C., Castillo, E. M., Savage, S., Maysent, P., ... & Longhurst, C. A. (2023). Ransomware attack associated with disruptions at adjacent emergency departments in the US. *JAMA Network Open*, *6*(5), Article e2312270. https://doi.org/10.1001/jamanetworkopen.2023.12270

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

Eichelberg, M., Kleber, K., & Kämmerer, M. (2021). Cybersecurity protection for PACS and medical imaging: Deployment considerations and practical problems. *Academic Radiology*, *28*(12), 1761-1774. https://doi.org/10.1016/j.acra.2020.09.001

Farringer, D. R. (2016). Send us the bitcoin or patients will die: Addressing the risks of ransomware attacks on hospitals. *Seattle University Law Review*, *40*, 937-985.

Feinstein, B. A., Bhatia, V., & Davila, J. (2014). Rumination mediates the association between cyber-victimization and depressive symptoms. *Journal of Interpersonal Violence*, *29*(9), 1732-1746. https://doi.org/10.1177/0886260513511534

Fox, A. (2022, November 7). St. Luke's Health reports data breach. *Healthcare IT News*. https://www.healthcareitnews.com/news/st-lukes-health-reports-data-beach

Gardella, J. H., Fisher, B. W., & Teurbe-Tolon, A. R. (2017). A systematic review and metaanalysis of cyber-victimization and educational outcomes for adolescents. *Review of Educational Research*, *87*(2), 283-308. https://doi.org/10.3102/0034654316689136

Georgiadou, A., Michalitsi-Psarrou, A., Gioulekas, F., Stamatiadis, E., Tzikas, A., Gounaris, K., ... & Askounis, D. (2021). Hospitals' cybersecurity culture during the COVID-19 crisis. *Healthcare*, *9*(10), Article 1335. https://doi.org/10.3390/healthcare9101335

Gill, J. (2022, October 17). St. Luke's Health record system is still offline 2 weeks after ransomware attack at parent company. *Houston Chronicle*. https://www.houstonchronicle.com/news/houston-texas/health/article/Record-systemoffline-St-Luke-s-hospital-Houston-17506573.php

Gordon, W. J., Fairhall, A., & Landman, A. (2017). Threats to information security—public health implications. *New England Journal of Medicine*, *377*(8), 707-709. https://doi.org/10.1056/NEJMp1707212

Healthcare Information and Management Systems Society. (2020). *2020 HIMSS cybersecurity survey*. https://www.himss.org/resources/himss-healthcare-cybersecurity-survey

Henson, B., Reyns, B. W., & Fisher, B. S. (2013). Fear of crime online? Examining the effect of risk, previous victimization, and exposure on fear of online interpersonal victimization.

Journal of Contemporary Criminal Justice, *29*(4), 475-497. https://doi.org/10.1177/1043986213507403

Holt, T. J., & Bossler, A. M. (2008). Examining the applicability of lifestyle-routine activities theory for cybercrime victimization. *Deviant Behavior*, *30*(1), 1-25. https://doi.org/10.1080/01639620701876577

Jalali, M. S., & Kaiser, J. P. (2018). Cybersecurity in hospitals: A systematic, organizational perspective. *Journal of Medical Internet Research*, *20*(5), Article e10059. https://doi.org/10.2196/10059

Jarrett, M. P. (2017). Cybersecurity—a serious patient care concern. *JAMA*, *318*(14), 1319-1320. https://doi.org/10.1001/jama.2017.11986

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

Lallie, H. S., Shepherd, L. A., Nurse, J. R., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of COVID-19: A timeline and analysis of cybercrime and cyber-attacks during the pandemic. *Computers & Security*, *105*, Article 102248. https://doi.org/10.1016/j.cose.2021.102248

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

Lee, C. S., & Wang, Y. (2022). Typology of cybercrime victimization in Europe: A multilevel latent class analysis. *Crime & Delinquency*. Advance online publication. https://doi.org/10.1177/00111287221118880

Leukfeldt, E. R., & Yar, M. (2016). Applying routine activity theory to cybercrime: A theoretical and empirical analysis. *Deviant Behavior*, *37*(3), 263-280. https://doi.org/10.1080/01639625.2015.1012409

Louderback, E. R., & Antonaccio, O. (2021). New applications of self-control theory to computer-focused cyber deviance and victimization: A comparison of cognitive and behavioral measures of self-control and test of peer cyber deviance and gender as moderators. *Crime & Delinquency*, *67*(3), 366-398. https://doi.org/10.1177/0011128720906116

Luna, R., Rhine, E., Myhra, M., Sullivan, R., & Kruse, C. S. (2016). Cyber threats to health information systems: A systematic review. *Technology and Health Care*, *24*(1), 1-9. https://doi.org/10.3233/THC-151102

Martignani, C. (2019). Cybersecurity in cardiac implantable electronic devices. *Expert Review of Medical Devices*, *16*(6), 437-444. https://doi.org/10.1080/17434440.2019.1614440

Martin, G., Martin, P., Hankin, C., Darzi, A., & Kinross, J. (2017). Cybersecurity and healthcare: How safe are we? *BMJ*, *358*, j3179. https://doi.org/10.1136/bmj.j3179

Middaugh, D. J. (2021). Cybersecurity attacks during a pandemic: It is not just IT's job! *Medsurg Nursing*, *30*(1), 65-66.

Milani, R., Caneppele, S., & Burkhardt, C. (2022). Exposure to cyber victimization: Results from a Swiss survey. *Deviant Behavior*, *43*(2), 228-240. https://doi.org/10.1080/01639625.2020.1806453

Miles, J. (2022, August 16). McKinney hospital, surgical centers targeted by group of Russian hackers. *CBS News*. https://www.cbsnews.com/texas/news/mckinney-hospital-surgicalcenters-targeted-by-group-of-russian-hackers/

Minnaar, A., & Herbig, F. J. (2021). Cyberattacks and the cybercrime threat of ransomware to hospitals and healthcare services during the COVID-19 pandemic. *Acta Criminologica: African Journal of Criminology & Victimology*, *34*(3), 155-185.

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

Neprash, H. T., McGlave, C. C., Cross, D. A., Virnig, B. A., Puskarich, M. A., Huling, J. D., ... & Nikpay, S. S. (2022). Trends in ransomware attacks on U.S. hospitals, clinics, and other health care delivery organizations, 2016-2021. *JAMA Health Forum*, *3*(12), Article e224873. https://doi.org/10.1001/jamahealthforum.2022.4873

Ngo, F. T., & Paternoster, R. (2011). Cybercrime victimization: An examination of individual and situational level factors. *International Journal of Cyber Criminology*, *5*(1), 773-793.

Ngo, F. T., Piquero, A. R., LaPrade, J., & Duong, B. (2020). Victimization in cyberspace: Is it how long we spend online, what we do online, or what we post online? *Criminal Justice Review*, *45*(4), 430-451. https://doi.org/10.1177/0734016820934175

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), Article 5119. https://doi.org/10.3390/s21155119

Partin, R. D., Meldrum, R. C., Lehmann, P. S., Back, S., & Trucco, E. M. (2022). Low selfcontrol and cybercrime victimization: An examination of indirect effects through risky online behavior. *Crime & Delinquency*, *68*(13-14), 2476-2502. https://doi.org/10.1177/00111287211061728

Perakslis, E. D. (2014). Cybersecurity in health care. *New England Journal of Medicine*, *371*(5), 395-397.

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), 23-29. https://doi.org/10.1097/HAP.0000000000000040

Pratt, T. C., Holtfreter, K., & Reisig, M. D. (2010). Routine online activity and internet fraud targeting: Extending the generality of routine activity theory. *Journal of Research in Crime and Delinquency*, *47*(3), 267-296. https://doi.org/10.1177/0022427810365903 Priestman, W., Anstis, T., Sebire, I. G., Sridharan, S., & Sebire, N. J. (2019). Phishing in healthcare organisations: Threats, mitigation and approaches. *BMJ Health & Care Informatics*, *26*(1), Article e100031. https://doi.org/10.1136/bmjhci-2019-100031

Pullin, D. W. (2018). Cybersecurity: Positive changes through processes and team culture. *Frontiers of Health Services Management*, *35*(1), 3-12. https://doi.org/10.1097/HAP.0000000000000038

Reisig, M. D., Pratt, T. C., & Holtfreter, K. (2009). Perceived risk of internet theft victimization: Examining the effects of social vulnerability and financial impulsivity. *Criminal Justice and Behavior*, *36*(4), 369-384. https://doi.org/10.1177/0093854808329405

Reyns, B. W. (2013). Online routines and identity theft victimization: Further expanding routine activity theory beyond direct-contact offenses. *Journal of Research in Crime and Delinquency*, *50*(2), 216-238. https://doi.org/10.1177/0022427811425539

Reyns, B. W., Fisher, B. S., Bossler, A. M., & Holt, T. J. (2019). Opportunity and self-control: Do they predict multiple forms of online victimization? *American Journal of Criminal Justice*, *44*, 63-82. https://doi.org/10.1007/s12103-018-9447-5

Saleous, H., Ismail, M., AlDaajeh, S. H., Madathil, N., Alrabaee, S., Choo, K. K. R., & AlQirim, N. (2023). COVID-19 pandemic and the cyberthreat landscape: Research challenges and opportunities. *Digital Communications and Networks*, *9*(1), 211-222. https://doi.org/10.1016/j.dcan.2022.06.005

Sethuraman, S. C., Vijayakumar, V., & Walczak, S. (2020). Cyber attacks on healthcare devices using unmanned aerial vehicles. *Journal of Medical Systems*, *44*(1), 29. https://doi.org/10.1007/s10916-019-1489-9

Sittig, D. F., & Singh, H. (2016). A socio-technical approach to preventing, mitigating, and recovering from ransomware attacks. *Applied Clinical Informatics*, *7*(02), 624-632. https://doi.org/10.4338/ACI-2016-04-SOA-0064

Slayton, T. B. (2018). Ransomware: The virus attacking the healthcare industry. *Journal of Legal Medicine*, *38*(2), 287-311. https://doi.org/10.1080/01947648.2018.1473186

Spence, N., Niharika Bhardwaj, M. B. B. S., & Paul III, D. P. (2018). Ransomware in healthcare facilities: A harbinger of the future? *Perspectives in Health Information Management*, *10*, 1-22.

Starks, T., & DiMolfetta, D. (2023, May 8). Dallas cyberattack highlights ransomware's risks to public safety, health. *Washington Post*. https://www.washingtonpost.com/politics/2023/05/08/dallas-cyberattack-highlightsransomwares-risks-public-safety-health/

Swede, M. J., Scovetta, V., & Eugene-Colin, M. (2019). Protecting patient data is the new scope of practice: A recommended cybersecurity curricula for healthcare students to prepare for this challenge. *Journal of Allied Health*, *48*(2), 148-156.

Tilley, C. (2022, November 15). ANOTHER hospital system goes down in cyberattack: Half a million records in Texas "are leaked." *Daily Mail*. https://www.dailymail.co.uk/health/article-11427607/ANOTHER-hospital-goescyberattack-Half-million-records-Texas-leaked.html

Tomaiko, E., & Zawaneh, M. S. (2021). Cybersecurity threats to cardiac implantable devices: room for improvement. *Current Opinion in Cardiology*, *36*(1), 1-4. https://doi.org/10.1097/HCO.0000000000000815

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

Turanovic, J. J., & Pratt, T. C. (2019). *Thinking about victimization: Context and consequences*. Routledge. https://doi.org/10.4324/9781315522333

Wasserman, L., & Wasserman, Y. (2022). Hospital cybersecurity risks and gaps: Review (for the non-cyber professional). *Frontiers in Digital Health*, *4*, Article 862221. https://doi.org/10.3389/fdgth.2022.862221

Williams, C. M., Chaturvedi, R., & Chakravarthy, K. (2020). Cybersecurity risks in a pandemic. *Journal of Medical Internet Research*, *22*(9), Article e23692. https://doi.org/10.2196/23692

Wilner, A., Jeffery, A., Lalor, J., Matthews, K., Robinson, K., Rosolska, A., & Yorgoro, C. (2019). On the social science of ransomware: Technology, security, and society. *Comparative Strategy*, *38*(4), 347-370. https://doi.org/10.1080/01495933.2019.1633187

Yar, M. (2005). The novelty of 'cybercrime': An assessment in light of routine activity theory. *European Journal of Criminology*, *2*(4), 407-427. https://doi.org/10.1177/147737080556056

Yeng, P. K., Fauzi, M. A., & Yang, B. (2022). A comprehensive assessment of human factors in cyber security compliance toward enhancing the security practice of healthcare staff in paperless hospitals. *Information*, *13*(7), Article 335. https://doi.org/10.3390/info13070335

Yeo, L. H., & Banfield, J. (2022). Human factors in electronic health records cybersecurity breach: An exploratory analysis. *Perspectives in Health Information Management*, *19*(2), 1-10.

Author Biographies

Peter S. Lehmann, Ph.D., is an Assistant Professor in the Department of Criminal Justice and Criminology at Sam Houston State University. His research interests include juvenile justice and delinquency, criminal sentencing, racial and ethnic disparities in punishment, school discipline and safety, and public opinion on crime and criminal justice policy. His recently published work has appeared in *Justice Quarterly*, *Journal of Research in Crime and Delinquency*, *Crime & Delinquency*, *Punishment & Society*, and other journals.

Alexander B. Kinney, Ph.D., is an Assistant Professor in the Department of Criminal Justice and Criminology at Sam Houston State University. His research unpacks the dynamics of social control in gray markets, uses automated text modeling algorithms to study the logics of deviant behavior, and theorizes punishment in a cross-historical context. Recently, his work has been published in *Social Problems*, *Poetics*, and *Sociological Inquiry*.

INSTITUTE FOR HOMELAND SECURITY

Sam Houston State University

The Institute for Homeland Security at Sam Houston State University is focused on building strategic partnerships between public and private organizations through education and applied research ventures in the critical infrastructure sectors of Transportation, Energy, Chemical, Healthcare, and Public Health.

The Institute is a center for strategic thought with the goal of contributing to the security, resilience, and business continuity of these sectors from a Texas Homeland Security perspective. This is accomplished by facilitating collaboration activities, offering education programs, and conducting research to enhance the skills of practitioners specific to natural and human caused Homeland Security events.

Institute for Homeland Security
Sam Houston State University

Kinney, A. B. & Lehmann, P. S. (2023) Mitigating Cybersecurity Threats to Hospitals and Healthcare Facilities. (Report No. IHS/CR-2023-1017). The Sam Houston State University Institute for Homeland Security. https://doi.org/10.17605/OSF.IO/NQR49