Medical Advisories as Deterrents in Healthcare Cybercrime

Nastaran Hadipour
Gupta College of Business
University of Dallas
Irving, USA
nhadipour@udallas.edu

Renita Murimi
Gupta College of Business
University of Dallas
Irving, USA
rmurimi@udallas.edu

***Abstract*— The use of Industrial Control Systems in healthcare offers several advantages in terms of ease of use, ease of access, remote configurability, and scalability across networks. However, medical ICS systems also pose significant risks in terms of an increased attack surface that could result in leakage of personally identifiable information, personal health information, and in extreme cases, malicious exploitation of devices and networks resulting in injury or death. This paper analyzes the entire dataset of ICS medical advisories published by the CISA, and covers a range of medical devices and systems. Our analysis of CISA's dataset of ICS medical advisories points to the evolution of complexity in the cybercrime threats confronting healthcare systems, as well as complexity in the networked environments within which healthcare operates.**

Keywords— medical advisories, industrial control systems, CISA, cybersecurity, healthcare, critical infrastructure

I. Introduction

Advisories have long been used as a policy initiative in diverse fields to deter undesirable behaviors and outcomes. Examples of advisories being used to inform, advise, and deter are found in government-issued travel advisories [1], terrorism communications [2], fishing industry compliance [3], pandemic advisories [4], cyberspace [5], and administrative law enforcement [6]. An advisory, at its core, is an outcome of a partnership between several organizations to create behaviors and actions that can prevent the actualization of some undesirable activity. Work in [7] describes two kinds of deterrents: latent and active. Advisories function as latent deterrents by providing defensive measures informing the intended audience of a vulnerability, and providing recommended solutions to address the vulnerability. The actions of the audience, guided by the advisories, serve to improve the security of both the individual and collective, achieving a larger goal of deterring malicious actors by improving the security of the entire system. This paper looks at how the Cybersecurity and Infrastructure Security Agency (CISA) advisories provide a proactive approach that incorporates latent deterrence to combat cybercrime in the healthcare cybersecurity industry.

Specifically, in this paper we examine the case of healthcare cybersecurity, which is one of the critical infrastructure sectors. In this paper, we performed a comprehensive examination of CISA's Industrial Control Systems (ICS) Medical Advisories (heretofore abbreviated as ICSMA) [8]. Established in 2018, CISA's central mission is to improve the resilience of critical infrastructure sectors against cybercrime threats. As part of this mission, CISA issues ICS advisories, providing timely information about vulnerabilities and mitigations for several critical infrastructure sectors. These advisories are categorized into six types: *Alerts, Analysis Reports, Cybersecurity Advisories, ICS Medical Advisories*, and *ICS Alerts*. In this paper, we focus on *ICS Medical Advisories* (ICSMAs). CISA's ICSMAs specifically address vulnerabilities in ICSs used in healthcare. These advisories are critical for organizations that managing healthcare infrastructure, as they offer essential guidance to ensure patient safety and continued functionality of critical medical equipment [9].

The contributions of this paper are twofold. First, this research has created a dataset consisting of CISA ICS medical advisories over the last eight years, incorporating factors such as vulnerability, risk, exploitability, and mitigation strategies. The systematic analysis of these factors offers a comprehensive view of security threats within the public health critical infrastructure. Second, this paper has mapped the vulnerabilities in ICSMAs to Open Worldwide Application Security Project (OWASP) security risks, and NSA mitigation strategies, providing a multi-faceted framework for understanding and addressing weaknesses. Together, these contributions can guide security assessments, prioritize remediation efforts, and inform the development of more robust, resilient ICS medical systems.

The rest of this paper is organized as follows. Section 2 describes related work focused on cybercrime threats in healthcare. Section 3 presents the methodology we adopted for analyzing the ICSMA database, and section 4 presents our findings from mappings the ICSMA content to various industry-standard taxonomies. Section 5 describes the insights and limitations of this study, and finally Section 6 presents socio-technical implications at the intersection of healthcare cybersecurity and critical infrastructure.

II. Related Work

Cybercrime in the healthcare industry is an outcome of weak security measures in complex networks as well as the relentless nature of threat actors. In [10], the authors examined the complexities surrounding cybersecurity vulnerabilities in medical devices with legacy systems, the need for rapid patching, and the critical nature of device functionality, as well as recommendations for improved collaboration between manufacturers, healthcare providers, and regulators to strengthen security measures. The security issues arising from integrating cloud computing and Internet of Things (IoT) technologies with Supervisory Control and Data Acquisition (SCADA) systems were examined in [11]. The value of

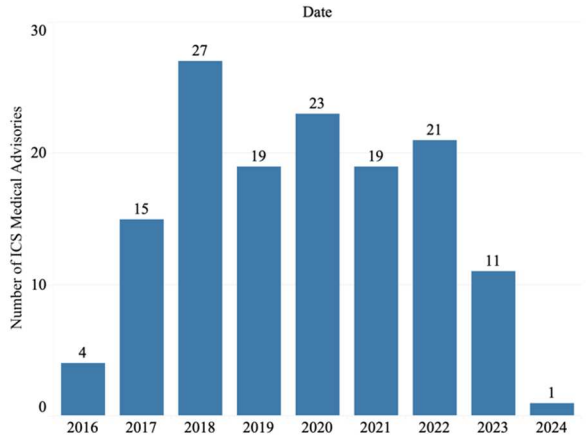

Fig. 1. CISA ICSMA advisory timeline

Personal Health Information (PHI) data to malicious attackers was studied in [12], where the high black-market value of sensitive medical data was shown to be a motivator for attacks targeting medical devices. Emergent cybersecurity risks associated with the increasing connectivity of implanted medical devices were studied in [13], where the authors illustrated real-world examples of suspected vulnerabilities, including related investigations by the Department of Homeland Security. Hospital cybersecurity was studied in [14] from an organizational perspective, where the authors emphasized that reducing endpoint complexity and ensuring alignment between stakeholders in the hospital environment would be more effective mitigation strategies than simply increasing allocated resources. Likewise, in [15], the authors emphasized that healthcare cybersecurity was not merely a technical challenge but a complex issue requiring organizational commitment and continuous adaptation to evolving threats by regularly performing a thorough risk assessment, implementation of robust security measures, and ongoing staff training. The role of the US Food and Drug Administration (FDA) involvement in healthcare cybersecurity was investigated in [16], where the authors analyzed FDA product summaries. Their findings showed that only a fraction of software-enabled devices explicitly addressed cybersecurity.

The preceding brief discussion on related work in healthcare cybersecurity shows the different approaches that are being used to analyze and mitigate cybercrime in healthcare. Our paper is the first effort that analyzes CISA ICS medical advisories and their role as deterrent in the critical infrastructure sector of healthcare.

III. Analysis of the CISA ICSMA Dataset

In this section, we present the methodology that we used for the ICSMA analysis. First, we generated a dataset containing the following factors: vendor, affected products, announcement date, vulnerabilities, CVSS score, attack method, exploit complexity, and public availability. The listing consists of a total of 140 Medical Advisories from March 2016 to Jan 2024, and the listing is expected to be ongoing as CISA discovers and shares information about advisories and alerts. Fig. 1 and Fig. 2 provide a summary of the number of ICSMAs by year, and the

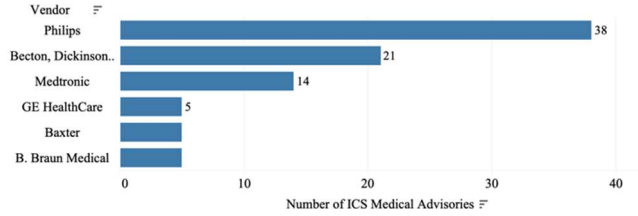

Fig. 2. Vendors featured more than five times in the ICSMA dataset

top vendors featured in the CISA ICSMA database. Before we proceed with the rest of the analysis, a brief description of Common Vulnerabilities and Exposures (CVEs) and Common Weakness Enumeration (CWEs) is in order.

First launched by the MITRE in 1999, the Common Vulnerabilities and Exposures (CVE) list, focuses on specific vulnerabilities in software and hardware [17]. Each vulnerability in the CVE list is assigned an identifier (e.g. CVE-2023-23397) and a description of affected products, severity score, and potential remediation steps. Since vulnerabilities can have varying degrees of impact, MITRE then developed the Common Vulnerability Scoring System (CVSS), a standardized method for rating the severity of security vulnerabilities. The CVSS score ranges from 0 to 10 and is calculated as a function of eight metrics. Subsequent work by the MITRE in vulnerability classification and categorization resulted in a complementary research discipline: weaknesses. Defining "weaknesses as errors that can lead to vulnerabilities", MITRE then developed the CWE in 2006 [18]. The main distinction between the CVE and the CWE is that the CWE offers details on the type of weakness, and the CVE details the vulnerability associated with a specific type of weakness. The CWE also lists the configuration flaws or faulty design choices that may lead to vulnerabilities. Similar to the CVE, each weakness is assigned a unique ID (e.g., CWE-79 for Cross-Site Scripting) with corresponding descriptions, consequences, and mitigations.

Each ICSMA frequently lists several vulnerabilities with different CVSS scores, but to account for worst-case scenarios, we consider the highest severity score in each report. The MITRE vulnerability severity scores fall under four categories: Low severity (0 - 4), Medium (4 - 7), High (7 - 9), and Critical Severity (9 - 10) [19]. From Fig. 3, we see that more than half of the vulnerabilities in the ICSMA dataset have a severity score higher than seven and need immediate attention. Fig. 4 illustrates the distribution of exploitability access methods, which CISA has differentiated based on the level of access an attacker possesses. Depending on the type of vulnerabilities, there might be more than one possible way of executing exploits on specific devices. *Remote attacks* are carried out over the internet or another network connection. The high number of remote exploits shows the dominance of network-based attacks and the critical need for enhanced network security, such as implementing firewalls, intrusion detection systems, and robust communication protocols.

On the other hand, attacks requiring *Physical Access* involve direct interaction with the medical device. The significant number of physical access incidents demonstrate the crucial

need for implementing physical safeguards and on-site security. ICSMA-19-022-01, for instance, warns about vulnerabilities

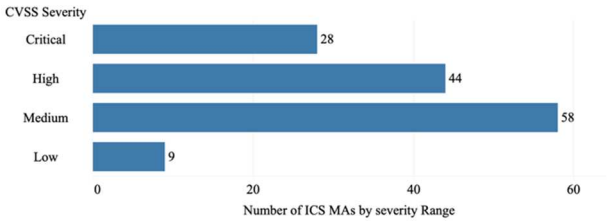

Fig. 3. Common Vulnerability Severity Scores in the ICSMA dataset

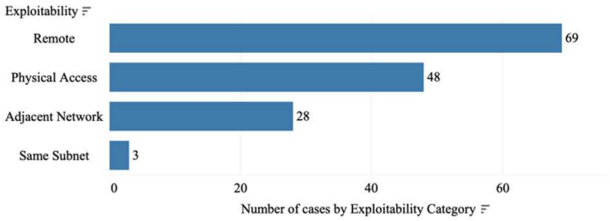

Fig. 4. Vulnerability Exploit Methods

found in Dräger's monitoring devices, which may cause exposure of device logs, denial of service through device reboots, and privilege escalation, allowing the attacker to reach the underlying operating system. In exploitability through *Adjacent Networks*, an attacker may target devices connected to the same network as the medical device but not necessarily on the same subnet. Attackers often compromise a weaker device and then move laterally within the network to gain access to the medical device. Network segmentation, isolating critical devices on subnets with strict access controls, can help mitigate this risk. For example, in the ICSMA-18-310-01 advisory, the Roche Diagnostics Point of Care Handheld Medical Devices features several weaknesses that may allow attackers in the adjacent network to gain unauthorized access via a service interface, modify system settings, or execute arbitrary code.

The final category of exploitability is that of attacks within the *Same Subnet,* which involves exploiting vulnerabilities within devices on the same subnet as the target device. This could mean exploiting misconfigured network devices or vulnerabilities arising from a lack of network segmentation. Although this category is featured on the fewest number of advisories, it still serves as a reminder that threats exist even within a localized environment. For instance, the Philips HDI 4000 ultrasound system, referenced in ICSMA-19-241-02, is built on an outdated, unsupported operating system, exposing ultrasound images and compromising image integrity. We also compare the public availability and skill difficulty of exploits found in advisories. The exploit availability chart in Fig. 5 indicates that about 15% of exploit codes are publicly available, while the remaining 85% don't have publicly known exploitation methods.

This emphasizes the importance of prioritizing vulnerabilities based on both severity and the likelihood of an attack. Even a less critical vulnerability can be exploited if the exploitation method is readily available. The exploit difficulty chart demonstrates that only 25% of vulnerabilities require sophisticated technical skills to exploit, which implies that the remaining 75% may be handled by low-skilled attackers. Fig. 5 emphasizes the need for a layered security approach because

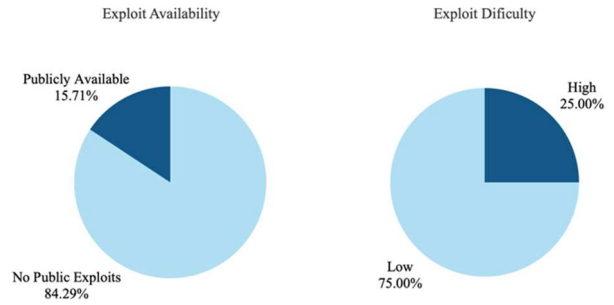

Fig. 5. Availability and Difficulty of Exploits

even if an exploit code exists, implementing strong defenses can make it difficult for attackers to exploit a vulnerability, regardless of skill level. The convergence of publicly available exploit codes and a low-skill barrier to entry creates a significant cybersecurity risk. If an attacker can easily find instructions and tools to exploit a vulnerability, even without advanced technical knowledge, it becomes much more likely that widespread attacks will occur. For example, ICSMA-19-311-02 warns about the vulnerabilities in Medtronic Valleylab FT10 and FX8 energy and electrosurgery products, including the use of hard-coded credentials, reversible one-way hash, and improper input validation. These vulnerabilities were found to be remotely exploitable via a low skill level required to perform exploits.

IV. Findings from the ICSMA Dataset

To better comprehend the scope of vulnerabilities, we mapped each ICSMA instance to two widely recognized cybersecurity frameworks: the OWASP Top 10, and NSA's Top 10 Mitigation Strategies.

A. Mapping the vulnerabilities in the ICSMA dataset to the OWASP Top 10

The Open Web Application Security Project (OWASP) provides information about the most critical web application security risks. These risks are relevant to Internet-connected medical systems that utilize web interfaces for communication, configuration, and data access. The most recent version currently available is OWASP Top 10: 2021, which we used in this paper [20]. Fig. 6 displays the distribution of OWASP security risks across different ICSMAs. Here, we focus on the top three frequently identified weaknesses in the ICSMA dataset, each including roughly one-quarter of advisories.

The A07 category of *Identification and Authentication Failures* emerged as the most common threat in medical devices. This category encompasses weaknesses in user identity verification and access control mechanisms. Common examples within this category include *CWE-287: Improper Authentication* and *CWE-798: Use of Hard-coded Credentials*. Exploitation of vulnerabilities in this category may allow a threat actor to gain unauthorized access to specific devices and associated data, potentially enabling data modification or manipulation of functionalities. For example, ICSMA-18-228-

01 involves the *Identification and Authentication Fail* (A07) security risk. This advisory reports several vulnerabilities in Philips page writer cardiographs, including hard-coded credentials and improper

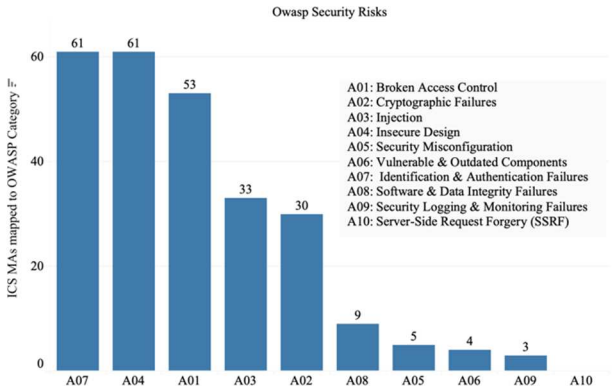

Fig. 6. Mapping Advisories to OWASP Top 10 Security Risks

input validation, which may allow an attacker to access and modify device settings. Next, the A04 category of *Insecure Design* was the second highest security risk found in the ICSMA dataset, highlighting the importance of improving design security in medical devices. This category refers to fundamental design flaws within the system that create security weaknesses, making them vulnerable to remote attacks regardless of user access. Examples of insecure design include *CWE-522: Insufficiently Protected Credentials* and *CWE-311: Missing Encryption of Sensitive Data*. This vulnerability can lead to complete device compromise, allowing manipulation of sensitive data and functionalities or even causing physical harm in devices like insulin pumps.

The third most frequently encountered security risk was the category of *A01: Broken Access Control*, which is also the OWASP's most critical risk in its top ten listing. This vulnerability arises when an application fails to properly restrict access to resources or functionalities based on user permissions. Examples *include CWE-284: Improper Access Control* and *CWE-200: Exposure of Sensitive Information to an Unauthorized Actor*. An example of A01 is ICSMA-20-079-01, which directly addresses *Broken Access Controls (A01)* security risk, which exists in the Insulet Omnipod insulin management system. This advisory warns about *CWE-284: Improper access controls*, which allow an attacker to gain access to the affected products to intercept, modify, or interfere with the wireless RF (radio frequency) communications to or from the product. This may allow attackers to read sensitive data, change pump settings, or control insulin delivery. CWE-284 is the second most common weakness found in ICSMAs, which fails to restrict access to resources from an unauthorized actor.

B. *Mapping the mitigations in the ICSMA dataset to the NSA's Top Ten Mitigation Strategies*

Next, we investigated the relationship between mitigations in the ICSMA dataset and the National Security Agency (NSA)'s Top 10 Mitigation Strategies. This list provide a set of ten categories of mitigation techniques centered on proactive defense approaches [21]. Fig. 7 demonstrates the distribution of NSA mitigation strategies across the entire ICSMA dataset in descending order of frequency. The top three mitigation strategies observed in the ICSMAs were as follows: *Update and*

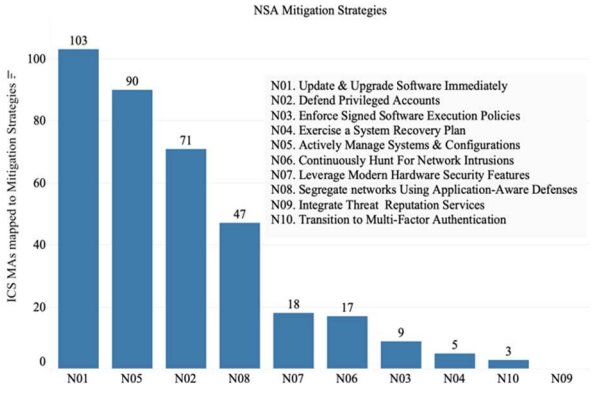

Fig. 7. Mapping Advisories to NSA Top 10 Mitigation Strategies

Upgrade Software Immediately (N01), Actively Manage Systems and Configurations (N05), and *Defend Privileged Accounts (N02)*. Below we describe the top three categories and their unique relationship to the ICSMA environment.

Update and Upgrade Software Immediately (N01) appears in nearly 75% of ICSMAs, implying a gap in security measures in the production of medical systems and devices. ICS medical devices often run specialized or legacy software with known vulnerabilities, and unpatched software is a primary entry point for cyberattacks. The second most frequent mitigation strategy was *Actively Manage Systems and Configurations (N05)*, which addresses the challenges associated with misconfigured devices or unapproved settings that can make them vulnerable. Complex medical device configuration and integration within the broader network, insecure default settings, unintended functionalities, and a general lack of adequate hardening can easily lead to exploitable openings for threat actors. The third most observed mitigation strategy in the ICSMA database was *Defend Privileged Accounts (N02)*. Since endpoint and networked medical devices hold sensitive patient data and control critical functions, privileged accounts such as administrator or root accounts must be tightly defended. Outdated privileged account management practices, hardcoded passwords, unencrypted credentials, and lack of granular access controls are all associated with defense flaws in privileged accounts.

V. Insights and Limitations

Our examination of the entire CISA ICSMA database offers several insights. First, each ICSMA is a collaborative effort featuring the contributions of cybersecurity research teams in the vendor organizations, third-party researchers, affiliated vendors and manufacturers, clinicians, hospitals, and patients. Many of the vendors are large international companies whose products are employed in healthcare around the world. Consequently, the CISA's ICSMA database has the potential to impact the security of systems, and the health and wellbeing of people around the world. Second, the ICSMA database has evolved in the kinds of information that are being profiled in each advisory, mirroring the evolution in other parallel open-source initiatives. Thus, current ICSMAs contain information

about specific vulnerabilities, weaknesses (and their families), severity scores, and mitigations, along with a cross-mapping

across several other databases such as the MITRE CVE and CWE. Finally, the ICSMA functions as a deliberate effort to improve the cyber resilience of the healthcare industry in cyberspace by providing a central resource for information dissemination about vulnerabilities and mitigations in software, hardware, and networking components. The next section presents the limitations of our study.

First, a few advisories had missing information, leaving gaps in our dataset. Specifically, the very first advisory issued by the CISA in 2016 did not mention the vulnerabilities found in the target devices, which prevented us from mapping the case to the OWASP top ten, or NSA's top ten mitigation strategies. Second, some existing vulnerabilities and related CWEs in the ICSMAs were not listed in OWASP's top 10 risks. To address these disparities, we explored the MITRE CWE database, which contains characteristics such as child/parent relationships for every CWE for all vulnerabilities not listed in the OWASP's top risk categories. Also, two vulnerabilities (CWE-17, CWE-254) that were present in the ICSMA dataset could not be mapped because MITRE has labeled their mapping as either being "*discouraged*" due to deprecation since 2019 (CWE-17) [42] or being grouped differently (CWE-254).

The third limitation is related to the evolving nature of the threat landscape. In our analysis, we mapped the ICSMAs to the OWASP Top 10: 2021 version, which was the most recent available version at the time of this writing. However, future versions of the top 10 might include newer security risks or even a change in the order of frequency of risk mapping and scoping to reflect the current security threat landscape. Finally, it is challenging to precisely delineate ICSMA mitigations with the corresponding NSA Top 10 mitigations, as some vulnerabilities could benefit from multiple mitigation strategies, and some vendor-recommended mitigations fall under multiple NSA mitigation categories.

VI. Discussion

Medical advisories are crucial for disseminating critical information, however, they can present unique socio-technical challenges. The complex interplay between the technical specifications of the advisory (such as the clarity of terminology and ontologies) and the social context (such as the real-world healthcare workflow and implementation, patient compliance, and ease of use) can lead to unpredicted consequences for confidentiality, integrity, and availability of healthcare cybersecurity. In this section, we will look at the socio-technical implications of medical advisories, the role of legal frameworks, and the interplay of artificial intelligence (AI) tools with the healthcare cybersecurity landscape.

A. Socio-technical implications of medical advisories

Advisories contain a trove of information about the causes, impacts, and prevention of vulnerabilities. In many cases, vendors mitigate the vulnerabilities through software updates, yet it is important to have proper communication with users if devices are not designed to get updates automatically. In other cases, user interaction is needed to mitigate the vulnerabilities. While major healthcare facilities may be equipped to address

ICS security as a collaborative effort between the cybersecurity team, healthcare providers, and patients, smaller healthcare facilities that may be under-resourced, such as those in rural areas, may be ill-equipped regarding the implementation of mitigation strategies for the healthcare cybersecurity. Thus, any mitigation should be performed with a consideration of the enterprise-level cybersecurity implications [24]. Complex cybersecurity jargon may be misinterpreted by clinicians, leading to gaps in effective communication and timely intervention.

Furthermore, endpoint patient devices, such as monitoring systems, insulin pumps and other handheld devices may require ongoing patient education regarding access control. Patients, themselves, may perceive these systems and devices differently with regard to their health and wellbeing, compared to IT administrators and clinicians, thus further warranting the need for audience-specific communication of advisories [25]. Protecting such devices from unauthorized access (e.g. remote or physical) is crucial to the individual's health and well-being, but users may not often possess the expertise to do so. Additionally, patient compliance with the security of medical devices may be suboptimal, which could lead to detrimental health outcomes. Further, the software and hardware life cycle may create issues surrounding obsolescence and sustainability. Thus, while medical advisories are crucial in disseminating information about cybersecurity threats to healthcare, they should be considered in light of broader socio-technical implications to meet the intended public health goals of the advisories and to ensure patient safety.

B. Legal Frameworks

A prominent framework for healthcare is the Health Insurance Portability and Accountability Act (HIPAA), which mandates strict security and privacy standards to handle PHI data. These mandates include provisions to include technical safeguards, administrative controls, and physical security measures. A notable legal framework is the HITECH Act, which enhances HIPAA by strengthening breach notification requirements and increasing penalties for noncompliance. Other regulatory bodies, such as the Food and Drug Administration (FDA) have been involved in developing regulations to improve medical device security. These include the FDA's pre- and post-market cybersecurity guidance, the Protecting and Transforming Cyber Health Care (PATCH) Act of 2022, as well as the provisions outlined in Section 524B of the Federal Food, Drug, and Cosmetic Act, added by the Consolidated Appropriations Act of 2023.

While non-compliance with these regulations can have significant legal implications ranging from substantial fines and reputational damage to product liability lawsuits, regulatory penalties, and even criminal charges in cases of negligence or malicious intent, there is room for improvement in the legal landscape surrounding ICS vulnerabilities. For instance, considering incentives for robust network design and stricter penalties for those who exploit vulnerabilities might be beneficial in securing healthcare networks and keeping malicious actors from targeting these critical systems.

Additionally, effective legislation regarding the responsibility of

medical device manufacturers in security against cyber threats might be a considerable next step in improving the cyber resilience of healthcare infrastructure [26].

C. Role of Artificial Intelligence

The rise of LLM tools over the past few years has revolutionized content generation in many sectors. These tools can generate text and software at alarming levels of sophistication. On the one hand, training AI models on historical advisory data can help identify subtle indicators of potential vulnerabilities that could lead to earlier identification of security risks, allowing healthcare providers to take swift mitigation measures. AI tools could also automate processes involved in vulnerability assessment and patch management. On the other hand, malicious actors could benefit from the easily accessible prowess of these tools to gather information about how to exploit vulnerabilities in medical devices. The abilities of AI-powered tools to parse terabytes of data can be leveraged to create specifically designed malware that triggers medical device malfunctions. This is only one such possibility of how AI tools can be misused, and it underscores the need for robust AI governance and ethical frameworks within the medical device security landscape.

VII. Conclusion

As healthcare becomes increasingly digitized and networked, the security of healthcare networks and data becomes crucial to its effective operation. This paper examined healthcare cybersecurity through a comprehensive examination of the listing of CISA's ICS medical advisories. The evolution of these advisories since the first listing in 2016 showed an increase in the complexity of attack vectors, vulnerabilities, and exploit techniques, which also parallels a corresponding increase in the complexity and attack surface of our broader networked environments. The insights presented in this paper from CISA's ICS medical advisory database can help the development of proactive cybersecurity strategies tailored to safeguard medical infrastructure and deter malicious attackers. Further, the insights obtained from such analyses can inform secure network design and policy development by facilitating collaboration among stakeholders in the healthcare industry, cybersecurity experts, and regulatory bodies.

References

[1] Beirman, D. (2006). A travel industry perspective on government travel advisories. In Tourism in turbulent times (pp. 309-320). Routledge.

[2] Freedman, L. (2005). The politics of warning: terrorism and risk communication. Intelligence and National Security, 20(3), 379-418.

[3] Mackay, M., Jennings, S., Van Putten, E. I., Sibly, H., & Yamazaki, S. (2018). When push comes to shove in recreational fishing compliance, think 'nudge'. Marine Policy, 95, 256-266.

[4] Bish, A., & Michie, S. (2010). Demographic and attitudinal determinants of protective behaviours during a pandemic: A review. British journal of health psychology, 15(4), 797-824.

[5] Mitchell, S. D., & Banker, E. A. (1997). Private intrusion response. Harv. JL & Tech., 11, 699.

[6] Winders, D. J. (2018). Administrative law enforcement, warnings, and transparency. Ohio St. LJ, 79, 451.

[7] Trujillo, C. (2014). The limits of cyberspace deterrence. Joint Force Quarterly, 75(4), 43-52.

[8] CISA ICS Medical Advisories. https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-137a

[9] CISA, "Cybersecurity alerts & advisories," https://www.cisa.gov/news-events/cybersecurity-advisories, 2024.

[10] P. Williams and A. Woodward, "Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem," Medical Devices: Evidence and Research, vol. 8, p. 305, Jul. 2015.

[11] A. Sajid, H. Abbas, and K. Saleem, "Cloud-assisted IoT-based SCADA systems security: A review of the state of the art and future challenges," IEEE Access, vol. 4, pp. 1375-1384, Mar. 31, 2016.

[12] L. Coventry and D. Branley, "Cybersecurity in healthcare: A narrative review of trends, threats and ways forward," Maturitas, vol. 113, pp. 48–52, Jul. 2018.

[13] J. G. Browning and S. Tuma, "If your heart skips a beat, it may have been hacked: Cybersecurity concerns with implanted medical devices," South Carolina Law Review, vol. 67, pp. 637–677, Mar. 2016.

[14] M. S. Jalali and J. P. Kaiser, "Cybersecurity in hospitals: A systematic, organizational perspective," Journal of Medical Internet Research, vol. 20, no. 5, p. e10059, May 2018.

[15] A. J. Coronado and T. L. Wong, "Healthcare cybersecurity risk management: Keys to an effective plan," Biomedical Instrumentation & Technology, vol. 48, no. s1, pp. 26–30, May 2014.

[16] A. D. Stern, W. J. Gordon, A. B. Landman, and D. B. Kramer, "Cybersecurity features of digital medical devices: An analysis of FDA product summaries," BMJ Open, vol. 9, no. 6, p. e025374, Jun. 2019.

[17] CVE, https://cve.mitre.org/

[18] CWE, https://cwe.mitre.org/

[19] CVSS scoring system calculator. https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator

[20] OWASP, "OWASP Top Ten," http://www.owasp.org

[21] National Security Agency, "NSA's Top Ten cybersecurity mitigation strategies," Mar. 2018.

[22] CWE-17 https://cwe.mitre.org/data/definitions/17.html

[23] CWE 254, https://cwe.mitre.org/data/definitions/254.html

[24] S. Jarjoui and R. Murimi, "A Framework for Enterprise Cybersecurity Risk Management," Advances in Cybersecurity Management, Springer, 2021.

[25] R. K. Murimi, S. Blanke, and R. Murimi, "A Decade of Development of Mental Models in Cybersecurity and Lessons for the Future," Springer Proceedings in Complexity, 2023.

[26] S. Jarjoui, R.M. Murimi, and R.K. Murimi, "Communities, Agency, and Resilience: A perspective Addressing Tragedy of the Cyber Commons", Cyber Defense Review, 2024.