Determining Internal and External Risks in a Medical Center

Cheryl Ann Alexander[1] and Lidong Wang[2,*]

[1]*Institute for IT Innovation and Smart Health, Mississippi, USA*

[2]*Institute for Systems Engineering Research, Mississippi State University, Mississippi, USA*

Abstract: An enterprise stores information in the cloud providing virtual storage of data as virtual memory. Cloud increases the enterprise's ability to offer data and service delivery, however it also increases the chances of a cybersecurity threat, and cyber risks, and increases the vulnerability of the enterprise to risks. It is important for the organization to perform risk management to determine cybersecurity risks. Cybersecurity is a key need for hospitals to manage threats of all types. Healthcare is notoriously vulnerable to cyber-attacks due to the valuable nature of patient information and the lack of updated medical equipment. In this paper, we discuss medical applications in cybersecurity, AI's role in cybersecurity, and risk management in medical cybersecurity.

Keywords: Risk, Cybersecurity, Threat, Attack, Vulnerability, Artificial intelligence (AI), Cloud, Healthcare.

INTRODUCTION

As an organization stores information in the cloud—the virtual storage of information acts as virtual memory. Cloud enables an organization to offer information and service delivery; however, it also creates opportunities for cyberattacks (Ho and Gross, 2021). Data from the cloud, from IoT devices or mobile devices, are a potential cyber target. Big data can be an asset, it needs to be protected against cyberattacks. A security breach that allows cyber criminals access to a huge volume of data could be disastrous (Dumitrescu *et al*., 2020).

MITRE Shield is a knowledge base developed to offer tools (used for countering cyber adversaries) to a defender. Shield techniques can be basic or advanced. Its foundational techniques include system activity monitoring, network monitoring, backup, and recovery, etc. (Fowler *et al*., 2020). MITRE ATT&CK is a worldwide accessible knowledge base. ATT&CK has become an effective tool across many cybersecurity disciplines (Strom *et al*., 2018).

Cyber-attacks can be a common problem within larger medical centers and small medical centers can suffer from cyber-attacks because they do not have the resources to identify and prevent cyber-attacks. It is key that medical centers use all the tools within the system for risk identification, risk analysis, and prevention so that patient data remains safe and protected from most risks. While protection of patient data is ideally targeted to be 100 percent protected from cyber risks; unfortunately, this is not possible due to the nature of medical equipment, patient data storage, and the use of mobile devices in patient care delivery.

A study on the electronic medical record (EMR) resistance from healthcare providers was finished, indicating that cyber-attacks are a main contributor to the resistance. It is also indicated that the policy of cyber-risk insurance helps mitigate the resistance to EMR systems (Samhan, 2020). Traditional evaluation frameworks evaluate risks according to the historical frequency as well as the severity of losses, which is effective for known risks and is not effective for many cyber risks because of the lack of historical data. A cyber risk classification and evaluation framework has been developed to quantify risks. This framework accounts for historical data, expert opinions, and known frameworks, which have been used in hospitals in a large city in Europe (Sheehan *et al*., 2021).

The primary purpose of the research in this paper is to deal with determining internal and external risks in a medical center. The authors discuss cyber threats and cybersecurity, the nature of AI in the practice of cybersecurity, and risk management for medical centers. Following these topics is a conclusion. The remainder of this paper will be organized as follows: the second section introduces cyber threats and cybersecurity; the third section presents artificial intelligence in cybersecurity and AI-based malicious activities; the fourth section introduces cyber risks and cybersecurity in medical and healthcare areas; the fifth section presents cyber risks in Charleston Regional Medical Center; and the sixth section is the conclusion.

*Address correspondence to this author at the Institute for Systems Engineering Research, Mississippi State University, Mississippi, USA;
E-mail: lidong@iser.msstate.edu

E-ISSN: 1929-4409/25

CYBER THREATS AND CYBERSECURITY

Cyber threats are at various levels and the most severe cyber threat can result in horrible damage to infrastructure or loss of lives. Table **1** shows the major types of cyber threats (Albahar, 2019). Cyber defense tools are multi-faceted, and their categories and activities are shown in Table **2** (Ho and Gross, 2021).

A risk analysis method for cyber-physical systems (CPSs) based on MARISMA (methodology for the analysis of risks on information systems, using meta-pattern and adaptability) and eMARISMA (an environment in the cloud). Table **3** shows categories of threats related to a CPS, with threats families and cases/examples (Rosado *et al*., 2022).

ARTIFICIAL INTELLIGENCE IN CYBERSECURITY AND AI-BASED MALICIOUS ACTIVITIES

Artificial intelligence (AI) helps detect new and sophisticated changes in attacks. AI enables the processing of a huge volume of data. An AI security system can learn over time to respond better to threats. AI has been used in cybersecurity, which is listed in Table **4** (Truong *et al*., 2020). However, there have been AI-based malicious activities that are shown in Table **5** (Truong *et al*., 2020).

CYBER RISKS AND CYBERSECURITY IN MEDICAL AND HEALTHCARE AREAS

Many hospitals in the United States are not prepared well for cyber risks and attacks. Risks can occur in the areas of electronic data, telemedicine/telehealth, medical devices, etc. Vulnerabilities associated with these areas, current risk management, and recommended strategies are shown in Table **6** (Wasserman and Wasserman, 2022). An attacker is aware that there is a huge volume of sensitive data, and that this kind of data should be readily accessible. Constant accessibility to the data causes vulnerabilities. Patient data should be shared easily because of the coordination requirement among the members of health teams. Interoperability has advantages for patients and healthcare providers but also brings cyber risks and attacks. Medical devices present opportunities for attackers to access data, change patient care, or infiltrate the network of a hospital. In addition, phishing

Table 1: Cyberattack Threats

Threat Types	Description
Service disruption	Malicious intrusion into computer systems, DDoS
Subversive cyber activities	Sophisticated intrusion into computer systems, involving modification of files & executables or defacing of legitimate websites
Cyber espionages	Penetrating sensitive organizational servers or government servers to steal data
An act of sabotage	Compromise of systems, leading to infrastructural damages
Full-scale cyber conflicts	Enable involving state players and leading to major loss of human lives

Table 2: Cyberdefense Tools and Activities

Defense Tools	Specificities of Knowledge
Password protection	Authentication, access control, encryption, remote administration
Anti-virus, anti-malware	Browser-based or systems-based anti-malware & popup blocker
Database knowledge	Prevention of SQL injections, inferential attacks, and attribution
Virtualization	Computer images, virtual machines
Physical security	Backup, recovery, digital forensics
Network penetration and defense	Network knowledge, Big Data analytics, intrusion detection, firewalls, penetration testing, port and IP scans and filtering
Systems and servers	Website knowledge, scripting, browser knowledge, honeypots, O/S knowledge, software updates and patches, coding integrity/quality, prevention of code injections & buffer overflow, etc.
Personnel security & training	Online reference, security clearance
Law and policy	Privacy law & security policy, corporate email & account policy, disaster recovery, business impact analysis

Table 3: Families and Types of Threats with Cases/Examples for the MARISMA-CPS Pattern

Families of Threats	Types of Threats	Cases/Examples
Disasters	Environment or natural disasters	Earthquakes, floods, fires
Outages	Network outage, system failure, failures of devices, loss of support services	Communication failure between non-IoT and IoT
Legal	Abuse of personal data, failure to meet contractual requirements, violation of rules & regulations/breach of legislation	Exposure or theft of clinical patient data
Physical attacks	Device destruction (sabotage), device modification	Theft of device & data
Failures/Malfunction	Third parties' failure, Software vulnerabilities	Software failures, device failures, overload, network component failures, insufficient maintenance, etc.
Damage losses (IT assets)	Data or information leakage	Noncompliance, physician and/or patient errors, medical system configuration errors
Eavesdropping/Interception/ Hijacking	Session hijacking, interception of information, a replay of messages, information gathering, Man-in-the-Middle	Skimming, hijacking to networks/sessions and medical devices
Nefarious activity/Abuse	Targeted attacks, malware, DDoS, exploit kits, information modification, attacks on privacy, counterfeit malicious devices	Phishing, social engineering, denial of service, medical device tampering, unauthorized access control, baiting and device cloning (RFID), etc.

is the most common delivery method for offenders to infiltrate healthcare systems with most cybercrimes being initiated via phishing emails (Wasserman and Wasserman, 2022).

Table 4: Applications of AI in Cybersecurity

Areas	Applications
Phishing/Spam detection	• Mail phishing detection • Web phishing detection • Spam mail • Spam on social networks
Network intrusion	• Anomaly detection • Intrusion detection
Malware detection	• Android malware • PC malware
Other	• Identifying domain names generated by domain generation algorithms (DGAs) • Countering advanced persistent threats (APTs)

Table 5: Malicious use of AI

Use of AI	Malicious Activities
Tools for attacking AI models	• Model Extraction • Poisoning the training data • Adversarial inputs
Autonomous intelligent threats	• Social engineering attacks • Strengthening malware/ AI-powered malware • Attacks against AI

Table 6: Associated Vulnerabilities, Current Risk Management, and Recommended Strategies for Electronic Data, Telemedicine/Telehealth, and Medical Devices

Aspects	Details
Vulnerabilities	Internet threats, out-of-date systems, constant accessibility, interoperability, lack of regulations, lack of resources, etc.
Current risk management	Detection and responses, technical measures, regulatory measures, insurance, etc.
Recommended strategies	Risk management, technical measures, group efforts, cybersecurity training, etc.

Internet of Medical Things (IoMT) devices are susceptible to cyber risks and attacks. Many of these devices are portable. Medical device vulnerabilities include 1) information exposure; 2) inappropriate authorization, privilege management, and access control; 3) improper input validation, 4) improper credential management and authentication, 5) missing encryption of sensitive data, 6) uncontrolled resource consumption, 7) path traversal, 8) cross-site request forgery, 9) stack and buffer overflow, and 10) cross-site scripting (Burke and Saxena, 2021).

An initiative to enhance the cybersecurity of a hospital Picture Archiving and Communication System (PACS) was implemented. The analysis of a hospital case study found the following losses (L1, L2, L3, and L4) as concerns across various stakeholders (Kaberuka and Johnson, 2020):

Table 7: Vulnerabilities and Losses at the System Level

Vulnerabilities	Losses
Inadequate separation of duties and permissive privileges for PACS users violate the least privilege principle	L1~L4
Lack of clear security policy	L1~L3
Circumventing web filters from the PACS system by unauthenticated proxy tools enlarges the attack surface	L1~L4
Inadequate end-point protection, out-of-date services on the PACS system, etc.	L1~L4

- L1: the loss of clinical planning, reputation, and time for treatment or inability to perform diagnosis in time,
- L2: the loss of the mission of hospital cybersecurity,
- L3: the loss of prevention behaviors,
- L4: the loss of sufficient clinical security.

The method in the case study facilitated finding vulnerabilities and losses within the hospital, which is shown in Table **7** (Kaberuka and Johnson, 2020).

The utilization of information and communication technology (ICT) helps hospitals deliver quality services but makes many ICT-based assets exposed to cyber-attacks. Figure **1** shows various ICT-based assets in a smart hospital (Coppolino *et al*., 2022). Risk assessment includes risk identification, risk analysis, and risk evaluation. It can be utilized by the Chief Security Officer of a hospital to detect a security breach that can destroy patients' health. A cyberattack can be launched against the contouring system: 1) the target of the treatment, and 2) organs at risk. An attacker gains access to the system and changes contouring delineations. The R&V (Record & Verify) system can be a target of a cyberattack. Patients' clinical data and the radiation treatment plan are utilized by the R&V system (Coppolino *et al*., 2022).

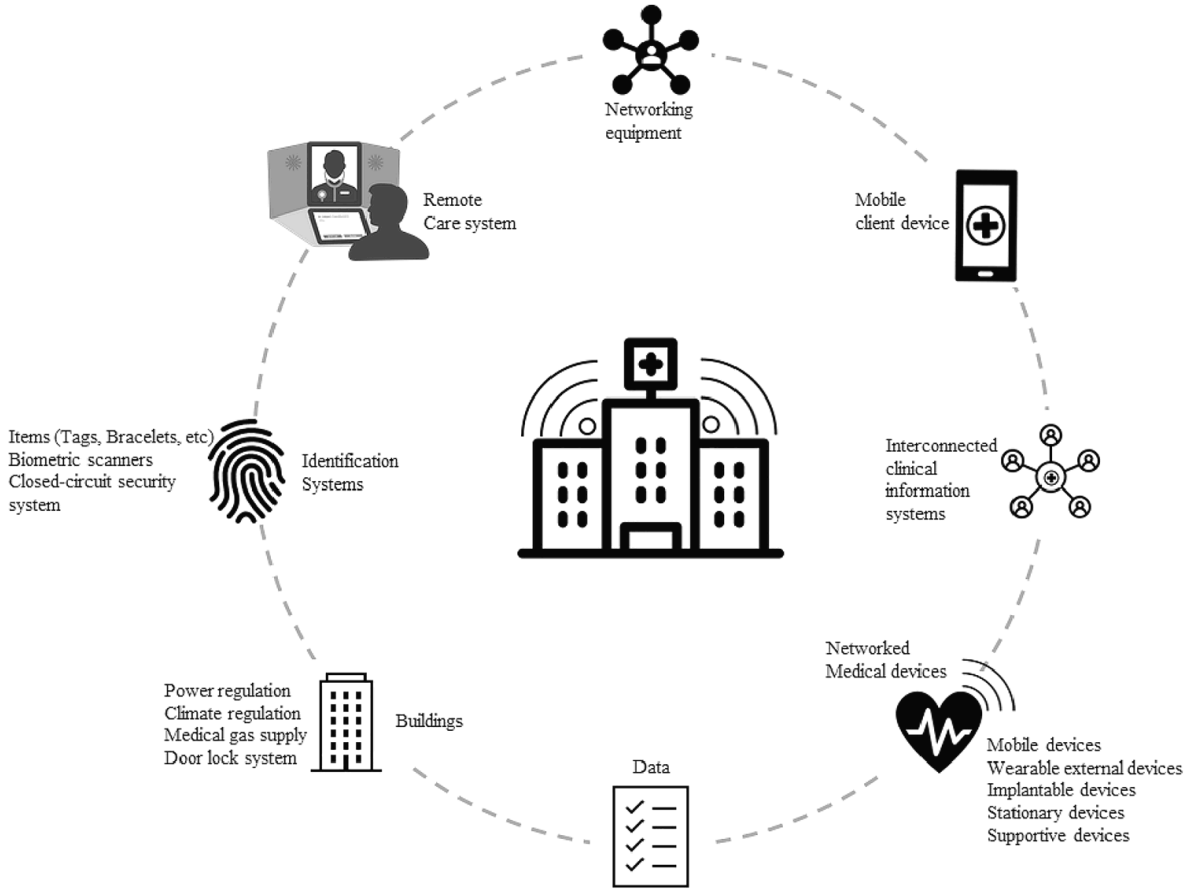

Figure 1: ICT-based assets in a smart hospital (Coppolino *et al*., 2022).

CYBER RISKS IN CHARLESTON REGIONAL MEDICAL CENTER

Charleston Regional Medical Center is a regional hospital in the US. Risks in the Medical center include internal and external risks. Internal risks are from patients, employees, and contractors. External risks are often from third parties and the cloud. Table **8** shows cyber risks in the Medical Center.

General vulnerabilities in the Medical Center include theft of patient information when discussing billing and coding appropriately, and insurance information by malicious actors when noting insurance information within the confines of payment. Threats are from malicious actors and internal actors such as staff, employees, clinicians, and providers who may be innocently accessing patient data but allow a wormhole for malicious actors to steal patient data.

Risks often occur when interacting with patients and others, such as unintended leak of patient information to third parties, speaking about patient information when on elevators, in break rooms, in the dining room, etc. Patient information possibly leaks when medicating, performing treatments, and giving oral reports by staff.

Risks can be leaking information about patients or other important information through supply chains such as pharmacy supply chains where parts of the medication are shipped from overseas and put together to make a medication in the Medical Center. Leaking of patient information by third parties is quite common, and when using medical equipment such as ventilators, IV pumps, and pharmaceutical tools, it requires a third party to verify patient information. Risks in administration and managers can be due to Ransomware, phishing emails, spam emails, and leaking patient information when billing, coding ICD-10, or discussing with providers and clinical staff.

Risks often exist in sensitive datasets and personally identifiable information (PII) uses, e.g., inadvertently speaking patient information on elevators, in emails, on phone calls to unverified third parties, and while in the patient's room about another patient. Sensitive datasets include patient general information, patient medical and clinical information, clinical trends, graphs, etc. The theft of patient information by internal and external malicious actors is a major risk or threat. There are risks in enterprise resource planning (ERP) in the cloud. For example, leaking patient information to third parties, and access of patient information by malicious actors who operate in the cloud. Risks can be in the Management Information System for Social Sector Programs (MISSP), e.g., continued risk of threats for malicious actors to steal valuable information about patients. The focus of threat actors includes stealing valuable patient information and selling it to the highest bidder. Foreign operations are often necessary, including supply chain, assembling medical equipment and pharmaceuticals, etc. Associated laws include the Health Insurance Portability and Accountability Act **(**HIPPA) and patient advocacy.

CONCLUSION

An enterprise uses the cloud for the storage of information. This virtual storage of data offers virtual memory for the enterprise. Virtual machines, therefore, make network switching enabled by virtual switches. As an organization stores information in the cloud—the virtual storage of information acts as virtual memory. By using cloud storage, organizations can offer data and services with delivery through virtual methods although opportunities for cyberattacks are created. While big data is an asset, it also needs to be protected from cyberattacks as well as data from the cloud, IoT devices, and mobile devices. A security breach can offer cyber criminals access to a huge amount of information which can prove disastrous to the organization. Cyber-attacks can result in the disarray of working systems, financial damage, or even the loss of life.

AI can detect cyber-attacks and a wide arrangement of security responses to predict and prevent cyber-

Table 8: Cyber risks in the Medical Center

Risks	Examples
Internal risks	Stealing passwords (e.g., computer passwords), passkeys to locked rooms, ID badges, and biometric information to pharmacy dispensation rooms
	Misuse of patient information by employees and contractors
External risks	Phishing emails, spam emails, Ransomware, and other cyber risks associated with email and patient information
	Theft of patient information by third parties through leaks in the cloud or in authorized uses of patient information

attacks. Many medical centers are vulnerable to security attacks, but many hospitals are unprepared for cyber risk identification and cyber-attack prevention. Risk management is a huge necessity for medical centers and risk identification and risk analysis are key to keeping attacks from happening. One reason this happens is that many hospitals do not have up-to-date equipment to identify, prevent, and recover from cyber-attacks. In this paper, the authors have reviewed and identified several risk factors and solutions to cyber-attacks within the hospital setting.

A comprehensive framework of cybersecurity includes risk monitoring, risk identification, risk assessment, risk analysis, and risk mitigation. AI can be used to continuously monitor medical network traffic, user behaviors, and system anomalies; recognize unusual patterns; and detect cyberattacks quickly. Existing vulnerabilities in healthcare include privacy issues, personal data abuse (ethical issues), technology weaknesses, etc. It is the responsibility of the healthcare IT team to maintain strict cybersecurity policies and updated technologies such as AI so that better services can be provided to identify and respond to risks efficiently in the future.

ACKNOWLEDGEMENTS

The authors would like to express thanks to Technology and Healthcare Solutions, USA for its help and support.

DECLARATION OF THE USE OF AI TOOLS

The authors declare that they did not use AI tools in writing this paper.

CONFLICT OF INTEREST

The authors would like to announce that there is no conflict of interest.

ETHICS

In this article, ethical principles related to scientific research articles are observed. The corresponding author confirms that both authors have read, revised, and approved the paper.

REFERENCES

Albahar, M. (2019). Cyber attacks and terrorism: A twenty-first century conundrum. *Science & Engineering Ethics*, 25(4), 993–1006. https://doi.org/10.1007/s11948-016-9864-0

Burke, G., & Saxena, N. (2021). Cyber risks prediction and analysis in medical emergency equipment for situational awareness. *Sensors*, 21(16), 5325. https://doi.org/10.3390/s21165325

Coppolino, L., Sgaglione, L., D'Antonio, S., Magliulo, M., Romano, L., & Pacelli, R. (2022). Risk assessment driven use of advanced SIEM technology for cyber protection of critical e-health processes. *SN Computer Science*, *3*, 1-13. https://doi.org/10.1007/s42979-021-00858-4

Dumitrescu Mihaela-Sorina, Paraschiv Dorel, Nițu Maria, & Florea Oana. (2020). Innovation and the evolution of cyber security Tools. *Junior Scientific Researcher, 6*(1), 64–71.

Fowler, C., Goffin, M., Hill, B., Lamourine, R., & Sovern, A. (2020). An introduction to mitre shield. Technical report. The MITRE Corporation.

Ho, S. M., & Gross, M. (2021). Consciousness of cyber defense: A collective activity system for developing organizational cyber awareness. Computers & Security, 108. https://doi.org/10.1016/j.cose.2021.102357

Kaberuka, J., & Johnson, C. (2020, June). Adapting STPA-sec for socio-technical cyber security challenges in emerging nations: A case study in risk management for Rwandan Health Care. In 2020 International Conference on Cyber Security and Protection of Digital Services (Cyber Security) (pp. 1-9). IEEE. https://doi.org/10.1109/CyberSecurity49315.2020.9138863

Rosado, D. G., Santos-Olmo, A., Sánchez, L. E., Serrano, M. A., Blanco, C., Mouratidis, H., & Fernández-Medina, E. (2022). Managing cybersecurity risks of cyber-physical systems: The MARISMA-CPS pattern. *Computers in Industry*, *142*, 103715. https://doi.org/10.1016/j.compind.2022.103715

Samhan, B. (2020). Can cyber risk management insurance mitigate healthcare providers' intentions to resist electronic medical records?. *International Journal of Healthcare Management*. https://doi.org/10.1080/20479700.2017.1412558

Sheehan, B., Murphy, F., Kia, A. N., & Kiely, R. (2021). A quantitative bow-tie cyber risk classification and assessment framework. *Journal of Risk Research*, *24*(12), 1619-1638. https://doi.org/10.1080/13669877.2021.1900337

Strom, B. E., Applebaum, A., Miller, D. P., Nickels, K. C., Pennington, A. G., & Thomas, C. B. (2018). Mitre att&ck: Design and philosophy. Technical report. The MITRE Corporation.

Truong, T. C., Diep, Q. B., & Zelinka, I. (2020). Artificial intelligence in the cyber domain: Offense and defense. Symmetry (20738994), 12(3), 410. https://doi.org/10.3390/sym12030410

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

Received on 06-11-2024 Accepted on 02-12-2024 Published on 23-01-2025

https://doi.org/10.6000/1929-4409.2025.14.01