Received 12/10/2025; Accepted 23/12/2025; Published 30/12/2025

Advanced Risk Assessment Techniques

Cheryl Ann Alexander cannalexander68@gmail.com
Institute for IT Innovation and Smart Health
Mississippi, USA

Lidong Wang lidong@iser.msstate.edu
Institute for Systems Engineering Research, Mississippi State University
Mississippi, USA

Corresponding Author: Cheryl Ann Alexander

Abstract

This paper introduces advanced risk assessment techniques that extend on theory, frameworks, and models, and presents risk assessments in healthcare. A case study regarding risk assessment in healthcare at Emerald Healthcare System is also presented. The case study includes risk assessment and compliance, data security, regulatory compliance, clinical care, and patient safety, risk assessment techniques or tools, and performing risk assessment in the healthcare system. Patient safety is the priority for all risk assessments in healthcare systems. Patient data and privacy are major concerns. A rigorous examination for compliance with healthcare data protection requirements should be a significant portion of the risk assessment. Training employees about cyber risks and having them be concerned about malicious actors is also a critical need for healthcare systems. When employees have buy-in, there is a much easier way to watch for malicious cybercriminals.

Keywords: Cyber risks, privacy, Compliance, cybersecurity, Internet of Things (IoT), Internet of Medical Things (IoMT), Failure mode and effects analysis (FMEA), Healthcare

1. INTRODUCTION

Information systems are often very susceptible to cyberattacks. Having a vigorous risk assessment is essential for preventing cybercriminals from having access to data. Risk assessment in healthcare information systems is crucial because healthcare systems are critically vulnerable to cyberattacks. The biggest risk in healthcare systems is not only safeguarding patient data and protecting privacy but also preventing legal action due to patient data breaches. A critical component of a robust cyber risk assessment is training employees and staff. Staff and employees should be trained on common cyber risks and how to avoid them. Many times, a serious breach of cyber risk assessment occurs when employees or staff are not aware of the many cybercriminals and how their approaches to patient data compromise private health information. Through a vigorous training program, employees can be educated on cyber risks and how to avoid common compromising situations.

Citation: Cheryl Ann Alexander and Lidong Wang. Advanced Risk Assessment Techniques. **Advances in Knowledge-Based Systems, Data Science, and Cybersecurity**.Research 2025;2(3):18.

Attackers have various knowledge and skill sets, which should be considered in risk assessment. It takes time to evolve a hazard. Not every attack can result in a hazard to a system. Developing an automated toolchain to integrate cyber and physical modeling, attack modeling, and penetration testing is necessary. An integrated and model-based method for the risk evaluation of cyber-physical systems (CPS) has been developed by employing a CPS testbed with industrial controllers and communication protocols [1].

An approach to risk assessment of individual CPS components (such as hardware and software) and a total cyber risk score was provided based on common vulnerabilities and exposures (CVE), which helps decide the most protected configuration for a developed CPS and elements to substitute or reconfigure a current CPS [2]. Researchers presented a dynamic Bayesian network method for the quantitative risk evaluation of the CPS based on the distribution network. A Bayesian model was created based on the structure of the network and the common vulnerability scoring system (CVSS) [3]. TABLE 1 [4], lists various assessment approaches.

Table 1: Evaluation Categories

Evaluation type	**Details**
Self-Evaluations	Evaluations are accomplished by people employed by an organization.
External or third-party evaluations	Evaluations are accomplished by external or third-party parties.
Audits	Internal audit: accomplished by a team outside a department, but within an organization. External audit: accomplished by outside contractors/consultants

CVSS has been a commonly utilized system for vulnerability scoring. TABLE 2 [5], shows the CVSS elements and the classification of their levels. FIGURE 1 [4], shows the life cycle of a continuous flow strategy regarding cyber resiliency and cybersecurity.

Table 2: The Elements of CVSS

Elements	**Classification of levels**
Attack vectors	Remote network Adjacent network Local
Attack complexity	High Medium Low
Authentication	None Single Multiple
Impacts of confidentiality Impacts of integrity Impacts of availability	None, partial, or complete

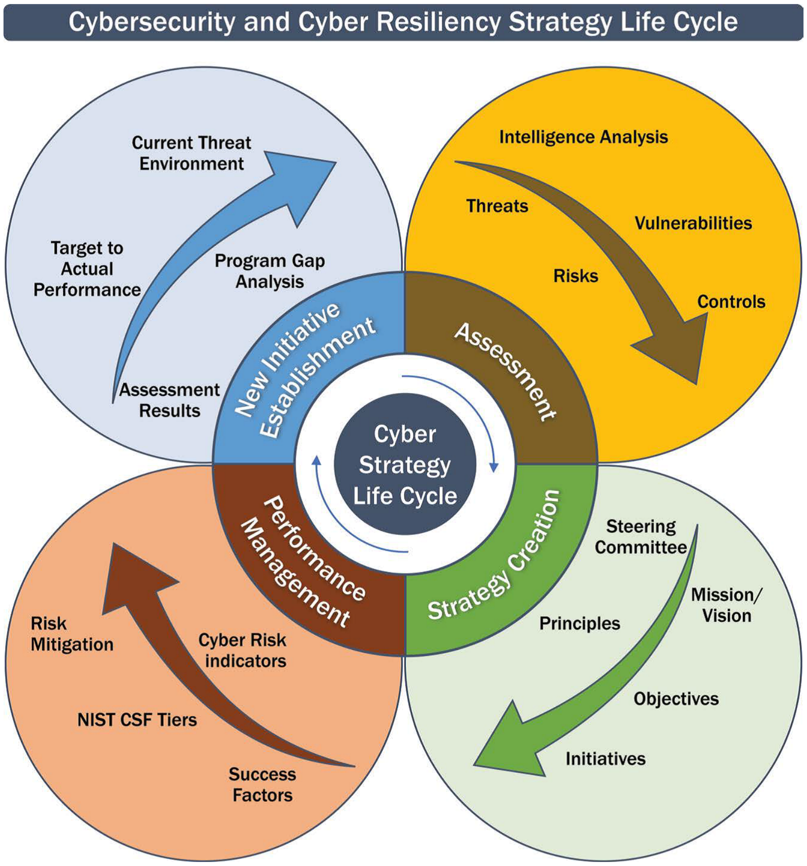

Figure 1: The Strategy Life Cycle Regarding Cyber Resiliency and Cybersecurity

This paper deals with advanced risk assessment techniques. The following is the arrangement of this paper: the second section introduces risk evaluation techniques that extend on theories, frameworks, and models; the third section presents risk assessments in healthcare; the fourth section is a case study regarding risk assessment in a healthcare system (including risk assessment and compliance in Emerald Healthcare System; data security, regulatory compliance, clinical care, and patient safety; risk assessment techniques or tools in Emerald Healthcare System; and performing risk assessment in Emerald Healthcare System); and the fifth section is the conclusion.

2. RISK EVALUATION TECHNIQUES THAT EXTEND ON THEORIES, FRAMEWORKS, AND MODELS

The Internet of Things (IoT) risks have been categorized into technical IoT risks, security IoT risks, privacy IoT risks, and ethical IoT risks. The risk evaluation theories of IoT include failure mode and effects analysis (FMEA) (identifying possible failures), fuzzy set theory (used in situations with imprecise or incomplete information), game-theoretic computing (for quantitative risk assessment in areas such as information security), cyber security game (quantitative assessment of digital security hazards), Dempster-Shafer theory (modeling uncertainties in risk evaluation) [6].

There are various risk evaluation frameworks. A hybrid risk assessment method and a standardized framework are suggested. Frameworks such as NIST, FAIR, and ISO 27005 have been commonly used. When a framework is performed, identifying information assets (especially identifying critical assets and ranking the assets based on criteria) is suggested. Risk assessment approaches include qualitative and quantitative assessments. Experts suggest that a mix of quantitative and qualitative assessments works best [7]. TABLE 3 [4], lists major evaluation vehicles, including frameworks, industrial standards, regulations, and models.

Table 3: Major Evaluation Vehicles: Frameworks, Industrial Standards, Regulations, and Models

Aspects	**Details**
Frameworks	NIST 800-53 Control Catalog: The most recognized control catalogs in cybersecurity (such as security and privacy controls).
	CERT$^{©}$-CRR: Assessing operating resiliency security practice.
	COSO ERM Framework: Expanding internal controls & providing a strong and far-reaching focus on ERM.
Industrial standards	PCI-DSS: Enhancing credit card cybersecurity globally.
	CPMI-IOSCO: Increasing the capability of financial market infrastructures to predict & respond to cyberattacks.
Regulations	NYDFS Cyber Regulation: It protects customers' information & IT systems of regulated entities
Models	FAIR: Factor Analysis of Information Risk (FAIR), quantifying & managing information risks.
	CMMI: Capability Maturity Model Integration (CMMI) is critical to understanding a cyber program's current state vs. an expected level.
	CM RQM: Scores & ranks initiatives according to the amount of risk reduction.
	PMBOK§: Authoritative in valuable practices of managing projects.
	CERT$^{©}$-RMM: A basis of a process-enhancement method for managing operational resilience.

A framework for risk assessment and mitigation was presented based on text mining. The framework offers the following functions: 1) cyber risk assessment for evaluating hackers' expertise (advanced, intermediate, beginner, or newbie); 2) cyber risk mitigation by calculating the financial impact of every combination (attack type, hacker expertise), ranking them, and prioritizing mitigation strategies [8].

A framework regarding a quantitative risk evaluation technique for cyber-attacks on cyber-physical power distribution systems (CPPDS) was proposed. The cyber-physical risk index was computed based on the Markov decision process (MDP). An altered MDP with the attack–defense game was provided. In the physical aspect, physical consequence calculation was conducted, and physical consequence values were obtained. In the cyber aspect, cyber-attack modeling was performed, and cyber consequence values were obtained. Based on the game and results, an optimum allocation plan for defense resources was achieved, as illustrated in FIGURE 2, [5].

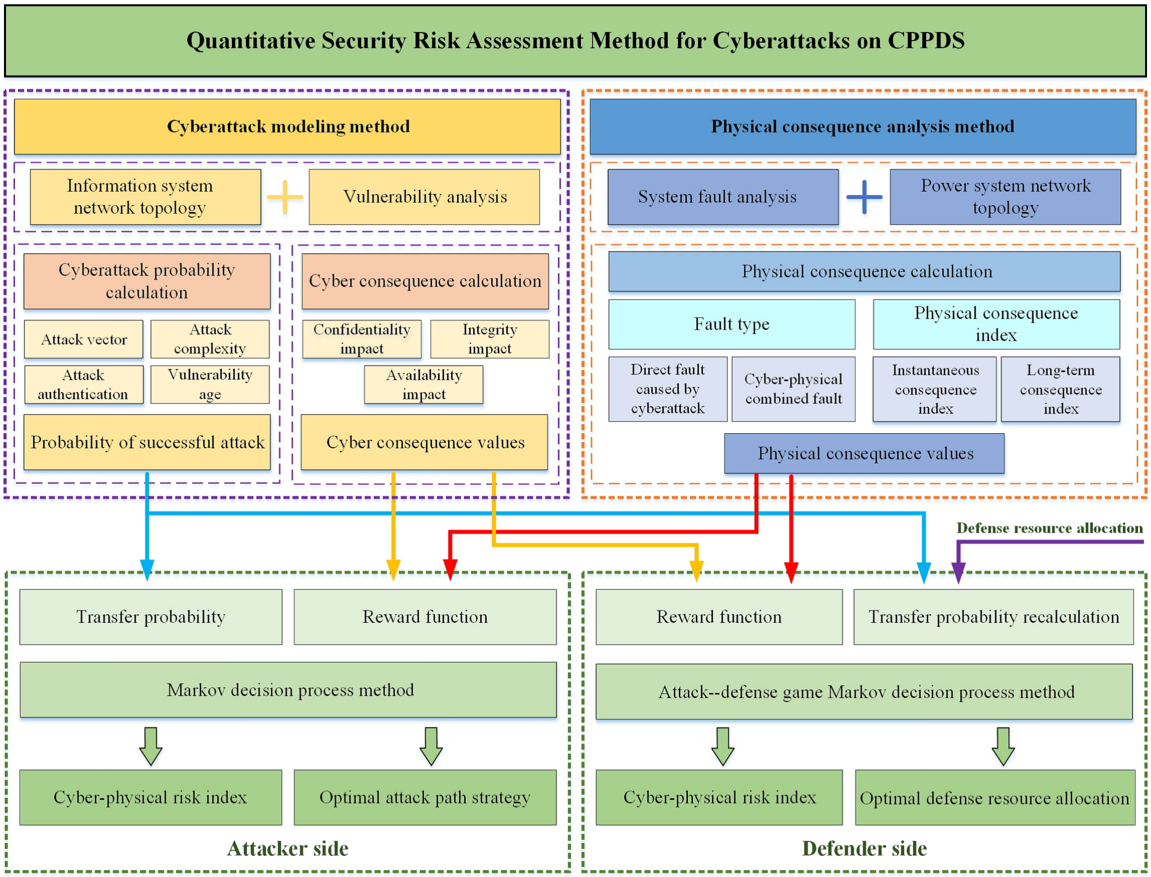
Quantitative Security Risk Assessment Method for Cyberattacks on CPPDS
Cyberattack modeling method
Information system network topology
Vulnerability analysis
Cyberattack probability calculation
Attack vector
Attack complexity
Attack authentication
Vulnerability age
Probability of successful attack
Cyber consequence calculation
Confidentiality impact
Integrity impact
Availability impact
Cyber consequence values
Physical consequence analysis method
System fault analysis
Power system network topology
Physical consequence calculation
Fault type
Physical consequence index
Direct fault caused by cyberattack
Cyber-physical combined fault
Instantaneous consequence index
Long-term consequence index
Physical consequence values
Defense resource allocation
Transfer probability
Reward function
Markov decision process method
Cyber-physical risk index
Optimal attack path strategy
Attacker side
Reward function
Transfer probability recalculation
Attack--defense game Markov decision process method
Cyber-physical risk index
Optimal defense resource allocation
Defender side

Figure 2: A Quantitative Risk Evaluation Approach to Cyber-attacks on a CPPDS

3. RISK ASSESSMENTS IN HEALTHCARE

A framework for risk evaluation based on Industry 5.0 for healthcare systems was presented. There are nine steps covered in the framework, including identification and conceptualization, security problems in healthcare, Industry 5.0-based security issues, the identification of factors, correlation analysis, risk assessment, validation, suggested measures, and review & revision [9]. COVID-19 revealed the need for more effective remote patient monitoring (RPM). FMEA is a useful method for identifying failures before they happen. Improved FMEA approaches to the risk assessment of RPM of COVID-19 were presented [10].

A cyber-risk evaluation method was presented for medical cyber-physical systems and the Internet of Medical Things (IoMT) that employ federated identity management (FIM) resolutions to handle users' identities. The vulnerabilities and cyber risks of healthcare IT systems, various medical devices, healthcare imaging systems, data capture and inventory systems based on radio frequency identification (RFID), etc., were considered in the cyber-risk assessment methodology. Healthcare assets and vulnerabilities in the assets are shown in TABLE 4, [11].

FIGURE 3 [11], illustrates an attack model that is a diagram of an attack tree of the FIM (Federated Identity Management) framework. SAML is an open standard language that is used to exchange authentication and authorization data. OAuth is an open standard that is used for access delegation.

The integration of the software bill of materials (SBOM) with vulnerability exploitability eXchange (VEX) can tackle supply chain opacity and allow an organization to shift from detecting theoretical vulnerabilities to prioritizing only actually reachable and exploitable vulnerabilities within a specific environment. Adopting the IEC 62443 Zone and Conduit model can transform a flat and vulnerable network into a segmented and resilient architecture (called structural defense). Organizational convergence to bridge physical and cybersecurity silos unifies traditionally separate teams with shared tech and processes for holistic management of risks. Aligning these elements with regulations, such as the U.S. Food and Drug Administration (FDA) and the European Union's Cyber Resilience Act (CRA), helps build a robust and thoroughly modern framework for healthcare resilience.

4. A CASE STUDY REGARDING RISK ASSESSMENT IN HEALTHCARE

4.1 Risk Assessment and Compliance in Emerald Healthcare System

Emerald Healthcare System is a healthcare corporation in the USA. Risk assessments incorporate several robust methods, including an internal audit, external audit, self-assessment, and software-based risk assessment. A vigorous risk assessment must include an overall evaluation of the IT infrastructure, electronic medical equipment, software systems, etc. The federal and state governments also ensure compliance, using standards, regulations, and rules; appointing healthcare governing bodies such as OSHA (Occupational Safety and Health Administration), AHRQ, etc., that not only safeguard patient safety but also protect sensitive patient data, avoiding legal and financial consequences for the healthcare organization. Threats to patient safety caused by medical and clinical errors and violations of patient data confidentiality can be mitigated by a robust cybersecurity framework. Healthcare operations have undergone significant changes in communication with the introduction of electronic health records, mobile devices, and the newest communication tools. Therefore, a compliance risk assessment should involve a review of policies and procedures and clinical practice regulations to guarantee compliance with relevant regulations and laws.

Table 4: Healthcare Assets and Vulnerabilities

Asset Group	Asset	Vulnerability
Infrastructure	Gateway	Lack of suitable segmentation & security architectures, unsuitable segregation
	Router	Anonymous proxies, buffer overflow, vulnerability on the routing path
	Assets of power supply & security	An insecure management protocol without encryption
Platforms & backend	Services based on the Web	Flaw in design, buffer overflow, & complex monitoring because of an excessive traffic gap between providers of services
	Cloud structure, set-up, & service	Data owners' misconfiguration in security control
Information	Patient medical records, medical images & pictures	Unsuitable storage with encryption & poor encryption for data transmission, lack of robust access control
Application & service	Data analytics & visualization	Path injection, code injection, SQL injection, etc.
	Device usage, device & network management	Default configuration & password, clear text of power distribution units in management protocols, without encryption in management packet exchanges
IoT devices (network protocols, perception layers, applicationlayers)	Web-based service, wireless sensor networks, RFID service, cloud infrastructure & service, data processing & computing, data mining applications	Buffer overflow; design flaw; default credentials; heart bleed bugs; low processing power; no authentication; poor configuration management; inadequate authentication & authorization; factoring RSA (a public-key cryptosystem) export keys; SNMP (simple network management protocol) agent default community string; lack of monitoring, physical security, and encryption (e.g., transport layer encryption).
IoMT devices	Software	Firmware or operating system vulnerability, 0-day vulnerability
	Hardware	Buffer overflow, design flaw, & low processing power
	Sensors & actuators	Commissioning without authorization, insecure key storage, data leakages due to a lack of robust encryption, etc.
Other equipment in IoT ecosystems	Embedded systems	Lack of mutual authentication between the server & clients
	Device for management	Insufficient policy, usability, or procedure flow
	Device for interface	Design mistakes, insecure interface, insufficient IT product specification, & unsuitable design of IT assets or business processes

continued..

Table 4: Healthcare Assets and Vulnerabilities

Asset Group	Asset	Vulnerability
Authentication for FIM framework (SAML, a standard): SAML protocols, profiles, & artifacts,	Customers' devices, organization devices, workstations, clinicians' workstations & similar devices	Susceptible to any attack, no authentication for service providers to utilize SAML assertions, no confidentiality & authentication requirements for a SAML assertion & response, no authentication requirement for SAML binding
FIM framework: OAuth (a standard)	OAuth protocols & associated software in applications	Lack of appropriate authentication for the verification of authorization servers, insecure transmission of query parameters in uniform resource identifier (URI), & CSRF (cross-site request forgery) bugs

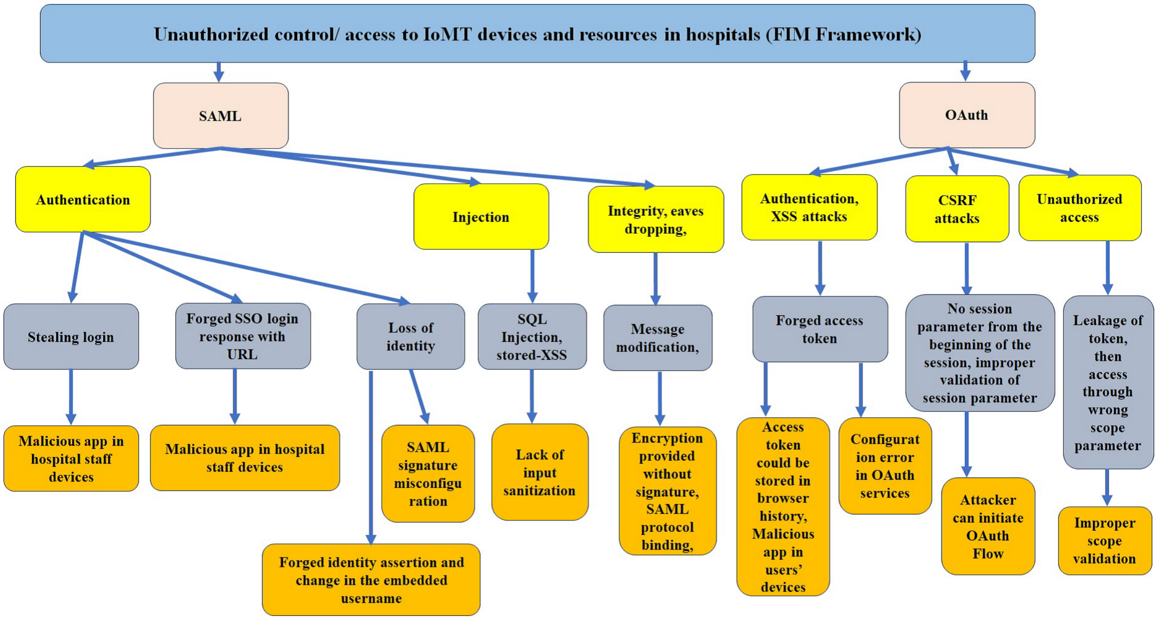
Unauthorized control/ access to IoMT devices and resources in hospitals (FIM Framework)
SAML
OAuth
Authentication
Injection
Integrity, eaves dropping,
Authentication, XSS attacks
CSRF attacks
Unauthorized access
Stealing login
Forged SSO login response with URL
Loss of identity
SQL Injection, stored-XSS
Message modification,
Forged access token
No session parameter from the beginning of the session, improper validation of session parameter
Leakage of token, then access through wrong scope parameter
Malicious app in hospital staff devices
Malicious app in hospital staff devices
SAML signature misconfigu ration
Lack of input sanitization
Encryption provided without signature, SAML protocol binding,
Access token could be stored in browser history, Malicious app in users' devices
Configurat ion error in OAuth services
Attacker can initiate OAuth Flow
Improper scope validation
Forged identity assertion and change in the embedded username

Figure 3: A Diagram of an Attack Tree of the FIM Framework

4.2 Data Security, Regulatory Compliance, Clinical Care, and Patient Safety

Emerald Healthcare System is increasingly relying on electronic health records (EHRs). Privacy, sensitivity, and data security are paramount. Risk assessments for this area are necessary to safeguard against data breaches and unauthorized access to patient records. A rigorous examination for compliance with healthcare data protection requirements should be a significant portion of the risk evaluation. Patient safety should be the priority for all risk assessments of the Emerald Healthcare System. Patient safety risks include diagnostic and clinical care errors, patient identification mistakes, surgical safety risks, and infection control. Healthcare risk assessments aim to identify these types of risks and work to mitigate any errors as quickly as possible. The Health Insurance Portability and

Accountability Act (HIPAA) is strictly enforced in Emerald Healthcare System to protect patients' sensitive data/information and guarantee its confidentiality, integrity, and availability.

4.3 Risk Assessment Techniques or Tools in Emerald Healthcare System

Emerald Healthcare System uses common risk assessment techniques or tools, including decision trees, risk matrices, and failure mode and effects analysis (FMEA). IT security professionals use the decision tree risk assessment tool to choose policies or choose between diverse action procedures. A risk matrix allows the cybersecurity professional to attach a quantitative risk value to any risks found. The risk matrix divides the quantitative risk value into diverse scales and segments numeric values for each probability and impact. This promotes scaling the values on a matrix and allows the IT member to scale the values on a matrix and assess the risk for each group of values. FMEA outlines all the ways a design, output, or procedure can fail.

4.4 Performing Risk Assessment in Emerald Healthcare System

Identifying data and assets: The healthcare IT security team of Emerald Healthcare System must identify key assets relevant to its risk assessment and should include patient data, human resources, facilities, technology assets, equipment, etc.

Risk identification: When the IT security team needs to identify risks, it is important to pinpoint any potential lapses in the Emerald Healthcare System. This can be done using direct observation, surveillance, surveys, data reviews, and algorithmic risk assessment tools.

Data analytics to measure risks: When using data analytics to measure risk, it is crucial to analyze the data and pinpoint the existing risks based on their possibilities and potential impacts. The IT security team should prioritize risk mitigation strategies and distribute resources accordingly.

Compliance review: It is also important to do a comprehensive compliance review to evaluate Emerald Healthcare System's adherence to specific healthcare rules, regulations, and standards, which can certainly identify how compliant the healthcare organization is.

5. CONCLUSION

Risk evaluation can be conducted by an audit, self-assessment, or external/third-party assessment. The risk assessment theories include FMEA, fuzzy set theory, game-theoretic computing, cyber security games, Dempster-Shafer theory, etc. There have been various risk assessment frameworks, including NIST, FAIR, ISO 27005, etc. Risk assessment can be quantitative or qualitative, and a mix of quantitative and qualitative assessment is often preferred. Patient safety is the priority for all risk assessments in healthcare systems. Patient data and privacy are major concerns. A rigorous examination for compliance (involving policies, regulations, procedures, etc.) with healthcare data protection requirements should be a significant portion of the risk assessment.

Acknowledgment

Thanks to Technology and Healthcare Solutions, Mississippi, USA, for its support.

Conflict of interest

None.

Ethics

There are no ethical problems in this paper.

References

[1] Tantawy A, Abdelwahed S, Erradi A, Shaban K. Model-Based Risk Assessment for Cyber Physical Systems Security. Computers & Security, 2020;96:101864.

[2] Northern B, Burks T, Hatcher M, Rogers M, & Ulybyshev D. Vercasm-Cps: Vulnerability Analysis and Cyber Risk Assessment for Cyber-Physical Systems. Information. 2021;12:408.

[3] Zhou B, Sun B, Zang T, Cai Y, Wu J, et al. Security Risk Assessment Approach for Distribution Network Cyber Physical Systems Considering Cyber Attack Vulnerabilities. Entropy, 2022;25:47.

[4] Siegel CA, & Sweeney M. Cyber Strategy: Risk-Driven Security and Resiliency. Auerbach Publications. 2020.

[5] Zhang Y, Ni M. Security-Oriented Cyber-Physical Risk Assessment for Cyberattacks on Distribution System. Applied Sciences. 2023;13:11569.

[6] Kandasamy K, Srinivas S, Achuthan K, Rangan VP. IoT Cyber Risk: A Holistic Analysis of Cyber Risk Assessment Frameworks, Risk Vectors, and Risk Ranking Process. EURASIP Journal on Information Security. 2020:1-18.

[7] Death D. Information Security Handbook. Packt Publishing. 2017.

[8] Biswas B, Mukhopadhya A, Bhattacharjee S, Kumar A, Delen D. A Text-Mining Based Cyber-Risk Assessment and Mitigation Framework for Critical Analysis of Online Hacker Forums. Decision Support Systems, 2022;152:113651.

[9] Baz A, Ahmed R, Khan SA, Kumar S. Security Risk Assessment Framework for the Healthcare Industry 5.0. Sustainability, 2023;15:16519.

[10] Parretti C, Tartaglia R, La Regina M, Venneri F, Sbrana G, et al (2022). Improved FMEA Methods for Proactive Health Care Risk Assessment of the Effectiveness and Efficiency of COVID-19 Remote Patient Telemonitoring. American Journal of Medical Quality, 2022;37:535-544.

[11] Huda S, Islam MR, Abawajy J, Kottala VNV, Ahmad S. A Cyber Risk Assessment Approach to Federated Identity Management Framework-Based Digital Healthcare System. Sensors, 2024;24:5282.