American Journal of Software Engineering, 2024, Vol. 7, No. 1, 1-7
Available online at http://pubs.sciepub.com/ajse/7/1/1
Published by Science and Education Publishing
DOI:10.12691/ajse-7-1-1

Creating a Comprehensive Assessment of Cyber Risks

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

[1]Institute for IT Innovation and Smart Health, Mississippi, USA
[2]Institute for Systems Engineering Research, Mississippi State University, Mississippi, USA
*Corresponding author: cheryl.alexander@techhealthsolutions.org

Received July 10, 2024; Revised August 11, 2024; Accepted August 18, 2024

Abstract New digital technologies have revolutionized the field of cybersecurity. Big data analytics, wearables, cloud computing, blockchain, Internet of Things, Internet of Medical Things, artificial intelligence, and machine learning are just a few of the new technologies. Sharing data and increasing accessibility and collaboration are critical to cybersecurity programs today. In healthcare, a risk assessment is key to guaranteeing the security and integrity of patient data including cyber-physical systems, networked equipment, supply chain management, and personal health information. In this paper, analysis and assessment of threats and cyber risks are presented. Software failures, software vulnerabilities, software updates, and outdated or unpatched software and applications are introduced. A comprehensive risk assessment for healthcare is introduced. A comprehensive risk assessment for a large medical center is presented as a case study. A critical list of cyber risks is presented according to the level of risk and how common the risk is. Software developers should consider cyber risks while designing software and applications.

Keywords: *cybersecurity, software, risk assessment, cyber risks, Internet of things (IoT), Internet of medical things (IoMT), blockchain, artificial intelligence (AI), machine learning (ML), healthcare*

Cite This Article: Cheryl Ann Alexander, and Lidong Wang, "Creating a Comprehensive Assessment of Cyber Risks." American Journal of Software Engineering, vol. 7, no. 1 (2024): 1-7. doi: 10.12691/ajse-7-1-1.

1. Introduction

Digital technologies, including Big Data analytics, mHealth apps, wearables, cloud computing, blockchain, Internet of things (IoT), Internet of medical things (IoMT), telemedicine, and artificial intelligence (AI)/machine learning (ML) have revolutionized healthcare services. Cloud computing aids in data sharing and storage and enhances accessibility and collaboration. Blockchain helps guarantee the security and integrity of medical records. IoT/IoMT devices connect healthcare systems and enhance remote monitoring and patient care coordination. Telehealth and telemedicine platforms connect geographical gaps and provide access to medical services and expertise. AI/ML can analyze huge medical information such as lab results medical images, and patient information to facilitate diagnosis and treatment. While these technologies have many benefits, they also bring new vulnerabilities and risks to healthcare systems and health data. For the mitigation of the risks, a solid framework is essential. This framework should include a comprehensive strategy of cybersecurity, strict access controls, secure network segmentation, regular assessments of risks, anomaly detection, data encryption, routine data backups, third-party vendor audits, threat intelligence sharing, incident response planning, and staff education [1].

The main outputs of risk analysis include 1) identification of assets that need protection, 2) identification of potential vulnerabilities, 3) identification of potential threats, 4) identification of the likelihood of potential risks and prioritization of risks, and 5) identification of treatments for risks [2]. Successful protection of crucial business processes can be achieved by using advanced SIEM (Security Information and Event Management) technology. It has been demonstrated that continuously monitoring security-relevant events and employing advanced correlation techniques help the SIEM to protect the key workflows of the hospital business processes from cyberattacks [3].

The objective of this paper is to deal with comprehensive risk assessment, focusing on healthcare applications to reduce the losses of lives and assets such as key medical devices, health data, and sensitive information. This paper first introduces the analysis and assessment of threats and risks for general organizations, then presents a comprehensive risk assessment for healthcare, and finally completes a case study of a comprehensive risk assessment for Charleston Regional Medical Center, a large medical center/hospital that serves patients in Jackson, Mississippi, USA.

2. Analysis and Assessment of Threats and Risks

There are four stages in the security framework. They are 1) risk evaluation and management, 2) security intelligence and analytics, 3) policies and procedures of

security, and 4) security monitoring. Comprehensive security solutions can be provided by combining common security frameworks such as COBIT, NIST Cybersecurity Framework, and ISO/IEC 27001:2013. COBIT is an internal control structure of practices, procedures, and policies to provide organizational results and detect, prevent, and improve undesirable actions [4].

Risk management is critical in handling cyber risks or threats in a cyber-physical system (CPS). It enables the identification of critical assets, vulnerabilities, and threats and determines appropriate proactive control measures for the mitigation of risks. A unified approach to cybersecurity risk management was proposed based on several methods that include fuzzy set theory for asset criticality, ML classifiers for risk prediction, and the comprehensive assessment model for assessing the effectiveness of available controls. It was demonstrated that the ML classifier's exemplary performance lies in predicting various risk types, including cyber espionage, denial of service (DoS), and crimeware [5].

Qualitative risk management and quantitative risk management have been used. Qualitative measures define risks according to the impact, severity, and likelihood of occurrence at various levels. They are usually faster and cheaper in the implementation since they are not numerically based. Quantification is the measurement of the quantity of something which when applied to cyber risks can help to break down a risk into different aspects that can be measured [6].

The methodology named “MARISMA” (methodology for the analysis of risks on information systems, using meta-pattern and adaptability) was developed that was supported by a technological environment called “eMARISMA”. The set of threats that may affect a system must first be identified to conduct a risk analysis. Table 1 shows a set of threats [7]. A comprehensive set of risks was identified and categorized to identify the risks of blockchain implementation. The fuzzy cognitive mapping technique was used to analyze the complex system of blockchain risk. Important risks of blockchain implementation and their ranking are listed in Table 2 [8].

Researchers have been inspired to develop a holistic and customized risk-based cybersecurity compliance assessment system (RC2AS) based on essential cybersecurity control (ECC). RC2AS presents a self-assessment tool that permits an enterprise to evaluate its compliance with the ECC and compute the compliance score using various approaches that meet the enterprise’s resources, needs, and criticality. The RC2AS tool guides the enterprise by handling its weaknesses, setting an appropriate plan to maintain what has been achieved, and suggesting potential solutions and approaches to improvement [9].

Threat modeling and risk assessment is a structured approach to detecting and prioritizing potential threats to a system, deciding the values of risks, and identifying potential mitigation. A threat analysis and risk assessment regarding sensors and data acquisition are shown in Table 3 [10]. A model-based risk assessment method named Yet Another Cybersecurity Risk Assessment Framework (Yacraf) was presented. Yacraf permits a comprehensive risk assessment for enterprises through the combination of two domains: quantitative risk assessment and model-based security analysis [11].

Table 1. A set of threats for a risk analysis

Family of Threats	Categories of Threats	Examples
Damage loss (IT assets)	Data/Sensitive information leakage	Physician and/or patient errors, medical system configuration errors, noncompliance
Eavesdropping/ interception/ hijacking	Network reconnaissance, information gathering, interception of information, man-in-the-middle, replay of message, session hijacking, communication protocol hijacking	Skimming, hijacking of networks/sessions and medical devices
Outages	Network outage, failure of a system, failures of devices, loss of support services	Failure of a health information system
Failures/malfunction	Third-party failures, software vulnerabilities	Software failures, network components failures, device failures, absence of audit logs
Nefarious activities/ abuse	Modification of information, targeted attacks, malware, Distributed denial-of-service (DDoS), attacks on privacy, exploit kits, counterfeit by malicious devices	Phishing, malware, denial of service, medical device tampering, social engineering, unauthorized access control, ransomware, viruses, baiting and device cloning in RFID
Physical attacks	Device destruction (sabotage), device modification	Theft of devices and data
Disasters	Environment disasters, natural disasters	Earthquakes, floods, fires
Legal problems	Abuse of personal data, failures to meet contractual requirements, violation of rules and regulations/breach of legislation	Exposure or theft of clinical patient data

Table 2. Risks of blockchain implementation and their ranking

Ranks	Risks
1	High investment costs
2	Privacy
3	Issues with contract laws
4	Chain defense
5	Compatibility risks
6	Working within the limitations of blockchain
7	User’s identity
8	Consensus mechanism and network management
9	Regulations
10	Lack of implementing transparent structures
11	Cryptography, key management, and tokenization
12	Consumption of high energy
13	Technology acquisition and implementation
14	Transaction accuracy and speed

Table 3. Threat analysis and risk assessment regarding sensors and data acquisition

Threats	Categories	Mitigation Strategy
Attackers try to modify the sensor data during communication.	Spoofing	Confidentiality, integrity
Attackers try to modify the sensor data at the source.	Tampering	Authenticity, integrity
Attackers try to modify the sensor node firmware/configuration.	Tampering	Authenticity, integrity
Attackers gain access to critical data, and leverage it to reverse-engineer the sensor firmware to design and deploy exploits.	Information disclosure	Confidentiality

3. A Comprehensive Risk Assessment for Healthcare

A medical CPS (MCPS) integrates human, cyber, and physical elements. A framework with the consideration of both the scheduling mechanism and security/privacy has been proposed. It is useful in healthcare applications. Table 4 shows the cybersecurity framework for an MCPS [12]. It covers various models and their components, functions, or responsibilities.

Table 4. A cybersecurity framework for an MCPS

Models	Components, Functions, or Responsibilities
Identification model	Policy management Asset management
Defense model	Access control Authentication Information protection Data security Preservation System hardening Cryptographic techniques
Diagnosing model	Awareness Monitoring Anomaly detection
Response/feedback model	Timely response Examination Coordination Upgradation Insecurity mitigation
Recuperation model	Coordination Recuperation
Trust model	Trust constructs Trust-based security mechanisms Trust management Identity access management Authentication Device inventory data
Risk model	Risk measure Risk level Risk management
Threat model	Threat analysis Threat modeling using Attack Trees Other threat modeling methods Threat modeling tools (e.g., security, MyAppSecurity, and Microsoft's free threat modeling tool)

The picture archiving and communications systems (PACS) infrastructure has been introduced to strengthen medical services. System-level vulnerabilities and losses are listed in Table 5, and the following losses have been identified in the hospital [13]:

- L1—loss of time, clinical planning, or reputation for treatment or inability to perform timely diagnosis
- L2—loss of cybersecurity missions or goals in a hospital
- L3—loss of prevention behaviors
- L4—loss of enough clinical security

Table 5. System-level vulnerabilities and losses

Vulnerabilities	Losses
Inadequate separation of permissive privileges and duties among PACS customers violates the least privileges principle.	L1, L2, L3, L4
Lack of clear security policies (i.e. guidelines and Internet policies among PACS customers) does not enhance ethical responses to cybersecurity issues	L1, L2, L3
Circumventing web filters from PACS systems by unauthenticated proxy tools increases the attack surface	L1, L2, L3, L4
Inadequate end-point protection or out-of-date services on PACS systems and other interactive systems of clinical information	L1, L2, L3, L4

IoMT, for example, wearable medical devices, can detect movement, positions, and vital signs. Such data or information helps improve the care quality for patients, even if they are far from a caregiver or physician. The security of medical devices is a major concern. To safeguard users, conventional risk assessment can be regularly conducted to detect possible security risks/threats, but this kind of method is not appropriate for handling advanced cyberattacks occurring in near real-time. Therefore, dynamic risk assessment is promising to handle inherent risks to patients utilizing IoMT [14].

IoT/IoMT has provided efficient and timely services in healthcare. Managing hospital data/records and monitoring patients remotely have made great progress due to IoT/IoMT. However, security and privacy are still a major concern, especially about personal and sensitive data. The National Institute of Standards and Technology (NIST) has proposed main goals for IoT risk assessment, which is shown in Table 6 [15]. Various types of risks regarding IoT/IoMT are shown in Table 7 [16].

Table 6. IoT risk assessment categories of NIST

Categories	Subcategories
Data protection	Provide secure back-up Sanitation of sensitive data Strong encryption capability of IoT devices Verify the identification of other computing devices
User privacy	Processing permissions management Disassociated data management Information flow management Processing permissions management
Device protection	Access management Vulnerability management Asset management Incident detection

Specifically, possible attacks in each of IoMT layers are given as follows [17]:

- Device tampering, sensor tracking, and tag cloning in the IoMT perception layer.
- Replay, eavesdropping, MiTM, DoS, and rogue access in the network layer.
- Session hijacking, cross-site request forgery, and cross-site scripting in the middleware layer.

- Ransomware, account hijacking, SQL injection, and brute force in the application layer.
- Information deception, Information disclosure, disruption due to DoS, and unauthorized access to the system due to sinkhole attacks in the business layer.

Table 7. Types of risks regarding IoT/IoMT

Types	Concerns	Concern for IoMT Devices
Security risks	Compromised data and data breaching during wireless transmissions	Attackers possibly gain access to patient data and change the data.
Privacy risks	Universal distribution of information, ubiquitous connectivity	Personal data sharing (sleep pattern, dietary habits, running routes, etc.)
Ethical risks	Ethical rules can be obstructed.	Adverse effects on individuals utilizing IoMT devices.

The participating nodes of IoMT networks generate, capture, and exchange huge sensitive and private data. IoMT is very vulnerable to security threats owing to the complexity and heterogeneity of the technology, privacy, and data/information sensitivity, fast-changing contexts, a multitude of stakeholders, and outdated infrastructure of Information and communications technology (ICT). A framework was proposed to improve trust and assist with decision-making in e-healthcare. It is based on the quantified risk assessment to assess risks related to three vulnerable areas in e-healthcare: the devices zone (data are generated), the network area (data are transferred over a multi-node transmission system), and the storage infrastructure (consisting typically of databases) [18].

A mobile medical applications (MMA) assessment module was established that enables an existing health technology assessment (HTA) process to be adapted for evaluating MMA. The adaptations should include making provisions for the analytical (reliability) validity, software updates, concerns about cybersecurity, evaluation of compatibility issues (e.g. operating systems and platform), incorporation of post-market performance data, as well as MMA-specific legal and ethical considerations [19].

The security risks of web-based hospital management systems (WBHMSs) have increased fast. Web application and software developers should consider these risks while designing web-based applications. In WBHMSs, the cybersecurity of patients' health information is very important. The risk evaluation relates to the secure integrity of the information following the Health Insurance Portability and Accountability Act (HIPAA). This covers securing the related financial records and the detection, evaluation, and prevention of data breaches. A hybrid technique named "Fuzzy Analytic Hierarchy Process-Technique for Order of Preference by Similarity to Ideal Solution (F-AHPTOPSIS)" was used to evaluate security risks in WBHMSs [20].

A popular modeling method, the attack tree, was employed in telemedicine with the attack success probability and attack occurrence probability as variables. Assessment and management approaches of risks appropriate for telemedicine were found; their benefits and potential limitations were evaluated. Attack Tree is a systematic approach to deciding the features of the system security according to all attacks to which a system is exposed. Seven areas of telemedicine security threats have been pinpointed: 1) patients or users, 2) telemedicine service providers, 3) telemedicine service providers, 4) Internet (public network), 5) home network, 6) gateway devices, and 7) the telemedicine system. This system manages all of the data of the patients who receive telemedicine services. It can introduce security risks/threats related to MiTM attacks, telemedicine app alteration/ forgery, malicious codes, and illegal network access via physical security checks circumvention. A gateway plays an intermediary role between a telemedicine system and a patient, exposing the system to security risks/threats related to rogue gateways and the theft/loss of gateways and MiTM attacks [21].

AI-based medical devices (AI-based MDs) have been undergoing great growth in medical applications. However, AI is deficient in meeting all HTA anticipations (safety, organizational impacts, costs, and economic assessment). HTA assessment criteria should be adapted because they ignore the significant specificities of AI-based MDs as follows: 1) the quality of clinical databases/datasets on which the device performance depends and which are not standardized and still of poor quality; 2) interpretability and explainability, which drive user acceptability; 3) reproducibility; and 4) interoperability. Studies on AI-based MDs have limitations and often lack robust, adapted, and complete evidence. Datasets with high quality are needed since output data can only be trusted if inputs are dependable. Available evaluation frameworks are not exactly developed to evaluate AI-based MDs. Frameworks should be adapted to evaluate the explainability, interpretability, safety, and cybersecurity of ongoing updates. Professional and patient acceptance, transparency, organizational changes, and ethical issues are necessary for the implementation of the devices. Specific HTA workflows and accurate evaluation tools should be developed to standardize the assessment of AI-based MDs. Such improvement can shape value-based healthcare for AI by producing reliable evidence and building confidence in advanced health technologies [22].

Healthcare organizations face advanced cyberattacks due to widely connected medical devices and sensitive and critical patient information. ML has been used for predicting possible security vulnerabilities in healthcare supply chain services. A method was proposed that utilizes ontology axioms to define essential concepts relevant to the overall healthcare ecosystem and to guarantee semantic consistency checking among such concepts. The conceptualization of healthcare cybersecurity utilizing an ontological approach offers the mechanism of better understanding the correlation between the security domain and the healthcare sector, while ML increases the accuracy of predicting vulnerability exploitability. It was shown that employing decision trees, linear regression, and random forest obtained good results in the prediction of vulnerability exploitability [23].

A standardized and collaborative approach to developing training programs, awareness campaigns, and information sharing on the types and nature of cyberattacks is essential to reinforce a healthcare organization against cyber risks/threats. Valuable practices

or recommendations from healthcare organizational experts must be promoted among healthcare stakeholders, including nurses, physicians, IT personnel administrators, and patients [24]. Table 8 [25] summarizes the measures that can be followed to improve cybersecurity in a hospital.

4. A Comprehensive Risk Assessment for a Medical Center

Patient data is the most critical asset in the medical center. Advanced medical equipment and networked medical equipment, including mobile assets such as phones, tablets, etc. are also used by providers and staff to provide care for patients. Networked medical equipment including ventilators, IV pumps, cardiac monitors, and other similar equipment are used in direct patient care. Billing data and insurance information are essential data that malicious actors are often targeting for cyberattacks. Intellectual property and operational systems are also targets for malicious actors.

Weaknesses can be found in mobile equipment used in patient care by providers and staff. Weaknesses include spotty mobile coverage, potential malicious activity by theft of devices, or password corruption. Some software may allow malicious actors to target these devices and steal patient information or other invaluable data.

Charleston Regional Medical Center is a large medical center/hospital that serves patients in Jackson, Mississippi, USA. Risks in the Medical Center are identified, and risk assessment is completed. The risk assessment is shown in Table 9. Various levels of risk impacts (critical, high, medium, and low) and likelihood (common, infrequent, and rare) for risk examples are identified and listed in the table, respectively. The risk assessment result is helpful for cybersecurity training, policy making, and reducing current and future losses.

Table 8. Measures taken by a hospital to enhance cybersecurity

Measures	Description	Threats
Updated equipment	Accounts for every piece of equipment in a hospital and its updated status	Theft or loss of equipment
Security of medical devices	Accounts for a medical device connected to the network and ensures that it is updated	Attacks against a connected medical device
Backup systems	Ensure that data are backed up continuously and that the size is increased after a backup	Ransomware
Systems for endpoint protection	Accounts for the size of unauthorized data transfers	Theft or loss of data
Email protection systems	Computes the number of spam filters used for each received e-mail	Ransomware Email phishing
Health information system (HIS) access control	Accounts for unauthorized access because HIS should not be accessed by unauthorized personnel	Theft/loss of data
Limitation of access to medical devices	Accounts for unauthorized access to medical devices	Attacks against a connected medical device
Policy of access management	Accounts for unauthorized access to a network	Accidental, unintentional, intentional data loss Ransomware
Cybersecurity policy implementation	Accounts for the policy availability regarding cybersecurity	Any threat
Routine staff training	Ensures that an employee has the training of cyber threats and cybersecurity once a year	Accidental, unintentional, and intentional data loss Email phishing

Table 9. Cyber risks and their measurement values in the Medical Center

Risks	Examples	Impacts	Likelihood
Internal risks	Stealing passwords (e.g., computer passwords)	Critical	Infrequent
	Stealing ID badges	Critical	Rare
	Intentional data loss	High	Rare
	Stealing biometric information to pharmacy dispensation rooms	High	Rare
	Misuse of patient information by employees and contractors	High	Infrequent
	Data leaks	High	Infrequent
	Accidental data loss	Medium	Common
	Stealing passkeys to locked rooms	Medium	Rare
	Outdated, unpatched software and applications	Low	Common
External risks	Theft of patient information by third parties through leaks in the cloud	Critical	Common
	Ransomware	Critical	Infrequent
	Device malfunctions	Critical	Common
	Orangeworm attacks: malware installed on a medical device such as MRI (magnetic resonance imaging) or X-ray machine	Critical	Rare
	Cyber-physical attacks: drug infusion pumps or insulin pump hack	Critical	Rare
	Cyber-physical attacks: telesurgery	Critical	Rare
	Cyber-physical attacks: heart rate monitors hack	Critical	Rare
	Web-based attacks: such as cross-site scripting or SQL injection targets a healthcare website	High	Common

Risks	Examples	Impacts	Likelihood
	Third-party or supply-chain attacks	High	Infrequent
	DDoS attacks	High	Infrequent
	Social engineering attacks	High	Common
	Account hijacking	High	Infrequent
	Theft of patient information by third parties through leaks in authorized uses of patient information	High	Infrequent
	Third-party data breaches	Medium	Common
	Open or vulnerable ports	Medium	Infrequent
	Malware	Medium	Common
	Other cyber risks associated with emails and patient information	Medium	Common
	Phishing emails	Low	Common
	Spam emails	Low	Common
Internal or external risks	The loss or theft of key equipment	Critical	Rare
	Attacks against networked key patient care equipment	Critical	Infrequent
	Billing data attacks	Medium	Common
	Attacks against non-essential medical devices	Low	Infrequent

5. Conclusion

IoT/ IoMT, AI/ML, blockchain, telemedicine, telehealth, etc. have promoted healthcare services greatly. While these advanced technologies have offered many benefits, they have introduced new vulnerabilities/risks/threats and other problems of cybersecurity. Comprehensive risk assessment, especially in the healthcare area, plays a vital role in fixing the problems of cyber risks. Both qualitative and quantitative assessments are very important. The completed case study of a comprehensive risk assessment for the Medical Center demonstrated a risk with low likelihood can have a critical impact on a hospital. A risk identified as a common likelihood and critical impact should be put the priority and remediated as soon as possible. Web application and software developers should consider cyber risks while designing web-based applications and software. The risk assessment result of the Medical Center helps to conduct cybersecurity training, make cybersecurity policies for hospitals, and reduce current and future losses in healthcare.

Acknowledgements

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

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

[1] Arafa, A., Sheerah, H. A., & Alsalamah, S. (2023). Emerging Digital Technologies in Healthcare with a Spotlight on Cybersecurity: A Narrative Review. *Information*, *14*(12), 640.

[2] Kpoze, A., Degila, J., Ahouandjinou, A., Houngue, P., Soude, H., & Wamba, S. F. (2023, August). Cybersecurity Risk Assessment for Beninese Power Grid SCADA system. In *2023 IEEE International Conference on Cryptography, Informatics, and Cybersecurity (ICoCICs)* (pp. 320-326). IEEE.

[3] 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.

[4] Alshammari, A. (2023). A Novel Security Framework to Mitigate and Avoid Unexpected Security Threats in Saudi Arabia. *Engineering, Technology & Applied Science Research*, *13*(4), 11445-11450.

[5] Kure, H. I., Islam, S., Ghazanfar, M., Raza, A., & Pasha, M. (2022). Asset criticality and risk prediction for an effective cybersecurity risk management of cyber-physical system. *Neural Computing and Applications*, *34*(1), 493-514.

[6] Healthcare Sector Cybersecurity Coordination Center (HC3). (2020). Quantitative Risk Management for Healthcare Cybersecurity, Report # 202005071030.

[7] 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.

[8] Samsamian, S., Hasani, A., Hakak, S., Esmaeilnezhad, T. F., & Khan, M. K. (2023). Comprehensive risk assessment and analysis of blockchain technology implementation using fuzzy cognitive mapping. *Computer Science and Information Systems*, (00), 39-39.

[9] Alfaadhel, A., Almomani, I., & Ahmed, M. (2023). Risk-Based Cybersecurity Compliance Assessment System (RC2AS). *Applied Sciences*, *13*(10), 6145.

[10] Siddiqui, F., Ahlbrecht, A., Khan, R., Tasdemir, S. Y., Hui, H., Sonigara, B., ... & Durak, U. (2023, October). Cybersecurity Engineering: Bridging the Security Gaps in Avionics Architectures and DO-326A/ED-202A. In *2023 IEEE/AIAA 42nd Digital Avionics Systems Conference (DASC)* (pp. 1-8). IEEE.

[11] Ekstedt, M., Afzal, Z., Mukherjee, P., Hacks, S., & Lagerström, R. (2023). Yet another cybersecurity risk assessment framework. *International Journal of Information Security*, *22*(6), 1713-1729.

[12] Priyadarshini, I., Kumar, R., Tuan, L. M., Son, L. H., Long, H. V., Sharma, R., & Rai, S. (2021). A new enhanced cyber security framework for medical cyber physical systems. *SICS Software-Intensive Cyber-Physical Systems*, 1-25.

[13] 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.

[14] Czekster, R. M., Grace, P., Marcon, C., Hessel, F., & Cazella, S. C. (2023). Challenges and Opportunities for Conducting Dynamic Risk Assessments in Medical IoT. *Applied Sciences*, *13*(13), 7406.

[15] Boeckl, K., Boeckl, K., Fagan, M., Fisher, W., Lefkovitz, N., Megas, K. N., ... & Scarfone, K. (2019). *Considerations for managing Internet of Things (IoT) cybersecurity and privacy risks.* Gaithersburg: US Department of Commerce, National Institute of Standards and Technology.

[16] Shanmugam, B., & Azam, S. (2023). Risk Assessment of Heterogeneous IoMT Devices: A Review. *Technologies*, *11*(1), 31.

[17] Kandasamy, K., Srinivas, S., Achuthan, K., & Rangan, V. P. (2020). IoT cyber risk: A holistic analysis of cyber risk assessment frameworks, risk vectors, and risk ranking process. *EURASIP Journal on Information Security*, *2020*(1), 1-18.

[18] Ksibi, S., Jaidi, F., & Bouhoula, A. (2023). A comprehensive study of security and cyber-security risk management within e-Health systems: Synthesis, analysis and a novel quantified approach. *Mobile Networks and Applications*, *28*(1), 107-127.

[19] Moshi, M. R., Tooher, R., & Merlin, T. (2020). Development of a health technology assessment module for evaluating mobile medical applications. *International Journal of Technology Assessment in Health Care*, *36*(3), 252-261.

[20] Alzahrani, F. A. (2021). Estimating Security Risk of Healthcare Web Applications: A Design Perspective. *Computers, Materials & Continua*, *67*(1).

[21] Kim, D. W., Choi, J. Y., & Han, K. H. (2020). Risk management-based security evaluation model for telemedicine systems. *BMC Medical informatics and decision making*, *20*(1), 1-14.

[22] Farah, L., Davaze-Schneider, J., Martin, T., Nguyen, P., Borget, I., & Martelli, N. (2023). Are current clinical studies on artificial intelligence-based medical devices comprehensive enough to support a full health technology assessment? A systematic review. *Artificial Intelligence in Medicine*, 102547.

[23] Islam, S., Abba, A., Ismail, U., Mouratidis, H., & Papastergiou, S. (2022). Vulnerability prediction for secure healthcare supply chain service delivery. *Integrated Computer-Aided Engineering*, (Preprint), 1-21.

[24] Nifakos, S., Chandramouli, K., Nikolaou, C. K., Papachristou, P., Koch, S., Panaousis, E., & Bonacina, S. (2021). Influence of human factors on cyber security within healthcare organisations: A systematic review. *Sensors*, *21*(15), 5119.

[25] Ahmed, M. A., Sindi, H. F., & Nour, M. (2022). Cybersecurity in Hospitals: An Evaluation Model. *Journal of Cybersecurity and Privacy*, *2*(4), 853-861.