Review Article

BIOMEDICAL Journal of Scientific & Technical Research

ISSN: 2574 -1241

DOI: 10.26717/BJSTR.2024.56.008926

Creating an Integrated Cybersecurity Plan for a Healthcare System

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

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

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

***Corresponding author:** Cheryl Ann Alexander, Institute for IT Innovation and Smart Health, Mississippi, USA

ARTICLE INFO

Received: May 22, 2024

Published: June 07, 2024

Citation: Cheryl Ann Alexander and Lidong Wang. Creating an Integrated Cybersecurity Plan for a Healthcare System. Biomed J Sci & Tech Res 56(5)-2024. BJSTR. MS.ID.008926.

ABSTRACT

Creating an integrated cybersecurity plan is critical for healthcare systems. Starting with a business continuity plan, it is essential to format asset management and a secure network infrastructure. Security awareness and identity and access management are critical. With the digitalization of healthcare systems, it is critical that healthcare leaders protect the data within their care. Therefore, the likelihood of a breach is greatly minimized as preparations are made to prevent and avert new attacks. This paper outlines software development security and integrated cybersecurity. It also outlines detection, response, mitigation, reporting, recovery, remediation, and lessons learned after a threat response in a healthcare setting as a case study. The knowledge that hackers and criminals are always one step ahead of health systems. It is essential that cyber programs be ramped up to include weaknesses and other data that individuals not working for the medical center are likely to ignore. In this paper, the full gamut of cybersecurity programs is described and laid out.

Keywords: Business Continuity; Secure Network Infrastructure; Security Awareness; Security Assessment; Security Testing; Software Development Security; Security Incident Report; Integrated Cybersecurity

Abbreviations: BCP: Business Continuity Plan; RFID: Radiofrequency identification; OR: Operating Room; EMR: Electronic Medical Record; IoT: The Internet of Things

Introduction

More significant than ever is cybersecurity awareness and planning in medical healthcare systems. With medical data being more valuable than ever, preparing for cyberattacks is essential and more critical than ever. With the digitalization of healthcare systems, it is critical that healthcare leaders protect the data within their care. The likelihood of a breach is therefore greatly minimized as preparations are made to prevent and avert new attacks (Javaid, [1]). Data from specific patients are gathered from multiple sources until a wide variety of data, including lab, notes from providers, nurses, staff, etc., is included and a picture of the patient's health is available to the cybercriminal. The rapid increase in digitalization and transfer of services to cyberspace leads to an increase in cyberattacks and incidents in cyberspace. Enterprises need to be prepared for multiple cyberattacks and global supply chains and healthcare facilities are under the threat of cybercrimes as private individuals are impacted and major disruption occurs. Significant financial and reputation damages occur to many facilities. Cybersecurity experts and teams are tasked with keeping information and Personally Identifiable Information (PII) secure and out of the reach of cybercriminals (Bukauskas, [2]). Cybersecurity breaches can affect the market value, reputation, and competitive advantage of the organization at risk. However, many studies have targeted cybersecurity management rather than the breach itself. Intrusion detection systems have emphasized how regulatory compliance can reduce the rates of and the number of occurrences of data breaches (Shaikh & Siponen [3]).

The knowledge that hackers and criminals are always one step ahead of health systems. It is essential that cyber programs be ramped up to include weaknesses and other data that individuals not working for the medical center are likely to ignore (Javaid [1]). The rise in healthcare technology has led the way to more and more sophisticated cyberattacks. A breach of information can include the loss of data, displacement of data, etc. At least two-thirds of organizations

have suffered a loss or theft of data since implementing the Electronic Medical Record (EMR). Most losses have been related to breaches or theft of data from portable devices (Bhuyan, et al. [4]). A cybercriminal accessed one of the servers in Charleston Regional Medical Center in the US by using a compromised username and password, leading to the theft of sensitive patient data pertaining to 21,836 patients. The following information was compromised in the data breach: names, dates of birth, addresses, phone numbers, social security numbers, credit card numbers with expiration dates, health insurance information, medical record numbers, etc. An incident management process often includes the following steps (Warsinske [5]): detection, response, mitigation, reporting, recovery, remediation, and lessons learned (debriefing).

Business Continuity Plan

A business continuity plan (BCP) is an approach employed to upgrade organizational flexibility, by improving the capacity of an enterprise to endure and continue business operations during a substantial disruption. BCP is essential not only for ensuring the availability of health and services, but also for supporting infrastructure and efficiency in any supply chain. A BCP requires data backup (off-site) and the capacity to retrieve it distantly (Tracey, [6]). Components of business continuity plans in healthcare systems include written disaster plans, backup communication, phone tree, the frequency with which plans are reviewed and updated (e.g., every year), plans orchestrated with regional and local agencies, pre-event cross-training of staff, the exercise frequency of a disaster (e.g., once every 3-6 months), etc. (Rebmann [7]). Suppose there is an information system outage or disruption in the Medical Center. In that case, Electronic Medical Records/Electronic Health Records (EMRs/EHRs), and the network infrastructure (devices, equipment, or hardware for network, storage, computing, etc.) are the recovery criticality. It is necessary for nurses to maintain patient safety if they do not have access to EMRs/EHRs due to the disruption.

Asset Management Program

Ineffective asset management in an operating room (OR) results in unsuccessful operation of resources, prolonged operational times, and risen costs. An analysis of acquired data helps quantify instrument use, procedure flow, performance, and avoidance of retained instruments. Radiofrequency identification (RFID) in the OR has been thought of as an approach to recognizing retained surgical items (Hendricks, et al. [8]). Hospitals persistently seek to enhance their business process flows and asset use and optimize procurement processes. Asset tracking management, followed by tracking medical staff and patients is a significant application for RFID in healthcare (Angeles [9]). Data is the primary asset in any medical center. Having a robust cybersecurity program is essential for protecting not only the patient data but also staff and data significant for the operation of the medical center. Data management involves data collecting, sharing, storing, using, and destroying when it is no longer needed. It helps stop data-related problems before they arise. As for information assets in the Medical Center, network-critical devices, servers, storage devices, medical databases, patient data, software (for access controls, diagnosis, medical image processing, patient monitoring), etc. are at a high level of significance.

Secure Network Infrastructure Plan

Network infrastructure devices include routers, firewalls, switches, servers, storage area networks, etc. Securing access to infrastructure devices, limiting unnecessary lateral communications, hardening network devices, physical or virtual separation of sensitive information, and implementing Out-of-Band management help secure network infrastructure (CISA, 2020). The Internet of Things (IoT) and the Internet of Medical Things (IoMT) have been applied in health care. (Table 1) (Alaba [10-12]) shows the layers classification of IoT. (Table 2) (Rangelov, et al. [13]) shows attack types, the layer targeted by an attack, and possible defenses or architectural measures in an urban IoT network. IoMT connects medical devices, health sensors, and health records to data platforms via wireless communication. A healthcare network is a kind of cyber-physical system. It includes IoT, embedded sensors, cloud computing, etc. There can be network security problems after a migration of the information system of a hospital to the cloud. Security problems can lead to 1) leakage of health data, and 2) loss or damage of the data (Gao [14]). Withthe intelligence of mobile terminal devices, a mobile healthcare network can present real-time communication and services in healthcare. However, security and privacy regarding healthcare data is a major concern. Ciphertext-policy attribute-based encryption can help protect security and privacy in a mobile healthcare network (Wang, et al. [15]). In Charleston Medical Center, blockchain helps not only to protect data but also to ensure that privacy standards such as the Health Insurance Portability and Accountability Act (HIPPA) are met (Kharatyan, et al. [16]).

Table 1: The Classification of IoT Layers.

Layers	Examples of Items
Physical layer	Temperature sensors, humidity sensors, smoke detectors
Network layer	Internet, cloud data centers, routing
Application layer	Smart healthcare, smart homes, smart transport

Table 2: Classification of Attack Types, the Layer Targeted by an Attack, and Possible Defenses or Architectural Measures in an Urban IoT Network.

Attack Types	Layers	Possible Defenses or Architectural Measures
Tampering	Edge and fog computing (E&FC)	Physical layer
Sleep deprivation or denial of sleep	E&FC	Physical layer
Node jamming or radio frequency interference	E&FC	Physical layer
Spoofing attacks	E&FC, machine learning (ML)/deep learning (DL)	Network layer
Distributed denial of service (DDoS)	E&FC, ML/DL	Network layer
Man-in-the-middle (MitM)	E&FC, ML/DL	Network layer
Sniffing attacks	E&FC	Application layer
Data theft	E&FC, blockchain	Application layer
Malicious code and database injections	E&FC	Application layer

Security Awareness and Training Program

Due to attacks and service disruption in the hospitals and clinical environment, there is a high demand for delivering security awareness and training programs (e.g., training to detect phishing emails) for healthcare professionals, with participants being nurses, doctors, admin personnel, and management teams. The programs, together with internal auditing effectiveness, are significant. A cooperative and standardized approach to the development of security awareness and training programs is expected to support hospitals against cyberattacks (Nifakos, et al. [17]). Allemployees in the Medical Center should complete universal training annually, including

1. Computers being covered with privacy screens.
2. Not chatting about patients in public places.
3. Regulations for Centers for Medicare & Medicaid Services and Medicaid.
4. Not reading information from charts if you aren't taking care of the patient.
5. Biometric screening, barcodes for medication safety.

Identity and Access Management Plan

Hospitals leverage identity and access management to minimize the disruption of clinical and administrative workflows. Secure access enables the rapid expansion of personnel working remotely (Gellert, et al. [18]). Blockchain is helpful for identity and access management in healthcare. It is useful to exchange and secure patient data and healthcare information in hospitals, pharmaceutical companies, diagnostic labs, and for healthcare providers (e.g., physicians, nurse practitioners, and physician assistants). It helps to detect medical takes and dangerous incidents. Identity and access control settings and access control settings should be maintained up to date (Warsinske, et al.[5]). It is necessary to update the identity and access status of people who leave the Medical Center or change departments or jobs within the center. There are many devices (e.g., computers, laptops, and biometric devices) in the Medical Center. If an employee does not work in the center anymore, the employee will be asked to return devices that had been issued to him/her for work.

Security Assessment and Testing Strategic Plan

Security assessment and testing (Warsinske, et al. [5]) in the Medical Center include

1) Regular vulnerability scans.
2) Reviews of user files and logs.
3) Testing the network system and hosts.
4) Assets tracking (such as medical devices, data extraction devices, and health data).
5) Assessment of cloud vendors and third-party service providers.
6) The susceptibility of employees to social engineering; and
7) Privacy concerns about the collected data.

It is helpful to periodically check system and network security by conducting penetration testing. Penetration testing is an approach to checking the security of a system or computer network through performing an attacking simulation (Satria, et al. [19]). Penetration testing in healthcare is helpful for detecting vulnerabilities of health information systems (including hardware/ medical devices, operation systems, application software and tools, etc.), and patient information and databases.

Software Development Security Plan

Software development security covers the security of the developmental environment, the security of software and components, application security, and the security of the developmental lifecycle (Warsinske, et al. [5]). There are possible troubles in vendor enterprises such as cyber theft. Research on developing a model of cyber

security challenges helps vendors' enterprises to recognize challenges in cyber security during software development (Khan, et al. [20]). (Table 3) lists some common security problems during the period of software design (Khan, et al. [21]). Tasks, challenges, and solutions during the period of the software design are listed in (Table 4) (Humayun, et al. [22]).

Table 3: Software Security Risks During the Software Design.

No	Security Risks
1	Lack of creating risk models during the software design
2	Lack of paying attention to obeying security design principles
3	Awareness lack in security design, guidance, and training
4	Inappropriate security design review and its verification
5	Lack of creating and maintaining the models of abuse cases and attacking patterns
6	Inappropriate security design documentation
7	Inappropriate conduction of the security review in design and architecture
8	Lack of creating the data flow diagram
9	Lack of requirements in security design
10	Lack of implementing security decisions (cryptographic protocols, mechanisms, frameworks, and services)
11	Lack of in-depth defense
12	Lack of access control and traceability
13	Lack of the encryption of design data and validation features
14	Inappropriate design audit logging features
15	Inappropriate assessment of risk from third-party components
16	Use of vulnerable components and sensitive application details

Table 4: Tasks, Issues/Challenges, and Solutions of the Design Phase.

Tasks	Issues/Challenges	Solutions
Identifying the assets of design	Creating requirements for design security	Keeping the design as simple as possible
Abstract specifications	Assessing risks in third-party component security	Applying false-safe default principle to guarantee that the failure of a task will avoid unsafe operations
Architecture design	Traceability	Applying access control to guarantee that the authorization of any entity is verified
Design of components	Access control	Providing the least privilege to keep a system from cyberattacks
Design of interfaces	Lack of in-depth defense	Following the least common principle to restrict access to shared resources
Database design	Awareness lack in security	Following the design principle of psychological acceptability for automatic incorporation of basic security
	Design flaws	• Applying the policy of in-depth defense (including multi-level security) • Performing the design review for the design validation

Development of a Security Incident Report in a Large Medical Center: A Case Study

Detection

In Charleston Regional Medical Center, biometrics is used to detect internal events; fingerprinting (one of the biometrics) is used to detect pharmaceutical events at the site of medication administration; and computer screening is used to prevent patients or third parties from reading or accessing the chart. Both the Chief Information Officer (CIO) and the Chief Security Officer (CSO) in the Medical Center received ransomware emails. The information security team checked the log-in records in the information system and recognized a compromised username and password on one of the servers. The data (patient data and research data) breach in the Medical Center was detected by the information technology team and reported to the CIO, CSO, and management team.

Response

As soon as the incident/data breach was confirmed and triaged, the Medical Center began to organize response activities. Preparation was made and actions were taken in time to mitigate the cyberattack and damage. Initial response plans (Warsinske, et al. [5]) can include the following actions:

- Disconnect the hardware that has been affected from the network, avoiding powering down and data (in volatile memory) loss.
- Utilize integrity checking to guarantee that copies have all original data.
- HIPPA (Health Insurance Portability and Accountability Act) secure emails—deidentified patient information

Mitigation

Mitigation is to stop an incident from getting worse. The first action is trying to perform the isolation or containing of the incident or data breach. The information security team and senior management in the Medical Center should determine whether the normal operational model is changed temporarily till the incident or data breach is completely resolved (Warsinske, et al. [5]). In addition, users are required to change their passwords, and all systems have the latest patches installed. It is also required to use multi-authentication including at least biometrics such as fingerprints in the access system. Access privilege policies are strictly implemented. Only authorized personnel can access patient data and research data. Privilege and authorization should be checked and audited on a regular basis in case some of the personnel changed their positions or left the Medical Center.

Reporting

Internal incident (data breach) reporting is given to both the CIO and the CSO in the Medical Center. The public relations officer will report the incident to the public. The center also needs to report the incident to customers (such as patients), partners (i.e., sister hospitals, etc.), service provider (i.e., access system) that associates with the incident, and related software/hardware suppliers or vendors. As a professional in security, how to handle breaches concerning personally identifiable information (PII) is a serious issue. Staff education and annual professional training are critical to reduce data breaches and mitigate cyberattacks on health data in the Medical Center. The professional training is provided to all employees in the Medical Center.

Recovery

A team with the proper training and skills of recovery should be formed before an incident. A recovery plan is started when the team responds to the incident. Services and capabilities are started to restore incrementally. It's easier to restore a system after an isolated incident rather than widespread problems. This kind of problem can typically be fixed by recovering prior system backups and replacing attacked files with clean ones (Warsinske, et al. [5]). The access system in the Medical Center is replaced by an updated version with the protection of security tools. There are many tasks in the recovery list. The recovery team decides the priority sequence according to the significance levels of the tasks and take recovery actions, following the priority sequence.

Remediation

Remediation means a restoration from reduced functionality to full functionality. The fix after remediation frequently corresponds to a restoration to full functionality. The remediation stage covers necessary activities to deal with impairments due to an incident or data breach. A hands-on approach is sometimes needed for severe problems or in the absence of a recent system backup. In this situation, it is needed to restore the system from a generic baseline or restoration point (Warsinske, et al. [5]). This leaves the Medical Center with a fresh and newly installed system. The information technology team takes a leading role in the remediation process after cyberattacks. In many situations, especially severe cyberattacks, all employees in the Medical Center should be involved in the remediation process.

Lessons Learned (Debriefing)

This is the final phase, including examining anything, seeing how an incident response process can be improved, going through incident management steps, and questioning or critiquing everything. This helps decrease the probability or impact of future data breaches or incidents. Lessons learned should be used in the training of awareness to avoid future incidents (Warsinske, et al. [5]). The lessons from the incident/data breach in the Medical Center lies in the failure to implement the cybersecurity practice of data protection standards outlined in HIPAA. Physicians, nurses, and only authorized individuals can access the data in the systems of the Medical Center. The lessons from the failure in practice can be added in the annual professional training.

Integrated Cybersecurity Methodology

Cybersecurity planning helps the selection and implementation of security controls to mitigate risks/threats. How to inform defensive decision-making to mitigate risks/threats was studied with a focus on making integrated, interdependent planning decisions (DuBois, et al. [23]). An integrated cybersecurity and cyber-awareness strategy was presented that consists of three main steps: 1) the assessment of cybersecurity attitudes & behaviors 2) self-diagnoses, and 3) learning/teaching activities. Table 5 shows some topics of training or learning/teaching programs in cybersecurity (Antunes, et al. [24]). An interoperable pipeline was offered to integrate external artificial intelligence (AI) tools with electronic health records (EHRs) (Afshar, et al. [25]). An integrated cybersecurity method and supporting tools for a healthcare information system have been proposed based on the capability

of integrating a medical practice system into a system of cyberattack detection, such as a SecurityInformation and Event Management System to congregate the security data from the components of systems, derive context for the analysis of use cases, and trigger the detection of anomalous behaviors (Coutinho, et al. [26]). It has been suggested that a completely integrated cybersecurity training platform should be created. The training platform needs more discreet, but realistic and comprehensive training in cybersecurity (Lee, et al. [27]).

Table 5: Some Topics Regarding Cybersecurity for Educational or Training Programs.

Main Groups	Topics
Common issues	Monitoring, information sharing, social engineering, malicious codes, abusive content, cyberbullying
Technical solutions	Software updates, antivirus, firewall, antimalware
Other issues	Passwords, fake news, social networks, incident handling, removable devices, blocking devices

Risk Analysis and Mitigation Recommendations

Regardless of what SDLC (software development life cycle) model is utilized, secure software development should be integrated throughout it. Vulnerabilities result from not only bugs due to coding flaws, but also weaknesses due to incorrect trust assumptions, security configuration settings, and obsolete risk analysis (Souppaya, et al. [28]). (Table 6) (Nelson, et al. [29]) shows the suggested practices of radiation oncology for the preparation and response to cyberattacks. Using the secure software development framework helps an organization to meet the following recommendations of software development (Souppaya, et al. [28]):

- Make sure that the people, technology, and processes have been prepared for the software development with strong security.
- Keep all the components of the software from unauthorized access and tampering.
- Develop secure software with the least vulnerabilities when it is released.
- Detect residual vulnerabilities after the software is released and give a proper response to deal with the residual vulnerabilities so that similar vulnerabilities will be avoided.

Table 6: Suggested Cybersecurity Practices of Radiation Oncology.

No	Suggestions
1	Keep offsite/ offline backup or printed copies of key records (e.g., clinical, or patient schedules) essential for treatment continuity.
2	Build necessary redundancies in hardware/software in case of hospital network shutdowns.
3	Develop the policies and procedures of outages in the hospital.
4	Execute disaster readiness exercises every year to discover possible problems.
5	Create a robust working relationship with the department of information technology department, for their support.

Conclusion

The rapid increase in digitalization and transfer of services to cyberspace leads to an increase in cyberattacks and incidents in cyberspace. Enterprises need to be prepared for multiple cyberattacks and global supply chains and healthcare facilities are under the threat of cybercrimes as private individuals are impacted and major disruption occurs. Significant financial and reputation damages occur to many facilities. With the digitalization of healthcare data, the loss of data and potential theft of data is great. Cybersecurity awareness is critical for healthcare systems. A business continuity plan is also essential for healthcare data to protect the data. Becoming cyber-aware is also key as hospital key personnel need to be aware of data loss. Password protection, biometrics, etc. are all protective devices for patient data. [30] Security assessment and testing for a secure plan is part of a robust program set by cybersecurity teams. Software security plans are also necessary for keeping up to date with cybersecurity programs. Integrated information security systems and cyberteams are necessary for ensuring that mobile data and healthcare data are protected. Risk identification and mitigation programs are necessary to prevent any theft of data. It is necessary to stay abreast of all threats and have a strong team prepared for every situation. Each team member must have the skills necessary for cybersecurity threats. Debriefing is probably the most essential skill which helps in forming future teams against future threats.

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.

References

1. Javaid M, Haleem A, Singh RP, Suman R (2023) Towards insighting cybersecurity for healthcare domains: A comprehensive review of recent practices and trends. Cyber Security and Applications 100016.
2. Bukauskas L, Brilingaitė A, Juozapavičius A, Lepaitė D, Ikamas K, et al. (2023) Remapping cybersecurity competencies in a small nation-state. Heliyon 9(1).
3. Shaikh FA, Siponen M (2023) Information security risk assessments following cybersecurity breaches: The mediating role of top management attention to cybersecurity. Computers & Security 124: 102974.
4. Bhuyan SS, Kabir UY, Escareno JM, Ector K, Palakodeti S, et al. (2020) Transforming healthcare cybersecurity from reactive to proactive: current status and future recommendations. Journal of Medical Systems 44: 1-9.
5. Warsinske J, Henry K, Graff M, Hoover C, Malisow B, et al. (2019) The Official (ISC) 2 Guide to the CISSP CBK Reference.
6. Tracey S, OSullivan TL, Lane DE, Guy E, Courtemanche J (2017) Promoting resilience using an asset-based approach to business continuity planning. SAGE Open 7(2): 2158244017706712.
7. Rebmann T, Wang J, Swick Z, Reddick D, delRosario JL, et al. (2013) Business continuity and pandemic preparedness: US health care versus non-health care agencies. American Journal of infection control 41(4): e27-e33.
8. Hendricks W, Mecca J, Rahimi M, Roja MR, Von Ballmoos MCW, et al. (2022) Evaluation of a Novel System for RFID Intraoperative Cardiovascular Analytics. IEEE Journal of Translational Engineering in Health and Medicine 10: 1-9.
9. Angeles R (2022) Understanding the RFID deployment at Sacred Heart Medical Center: Using technology-organization-environment framework lenses. Procedia Computer Science 196: 445-453.
10. Alaba FA, Othman M, Hashem IAT, Alotaibi F (2017) Internet of Things security: A survey. Journal of Network and Computer Applications 88: 10-28.
11. Hassija V, Chamola V, Saxena V, Jain D, Goyal P, et al. (2019) A survey on IoT security: application areas, security threats, and solution architectures. IEEE Access 7: 82721-82743.
12. Liang X, Kim Y (2021 January) A survey on security attacks and solutions in the IoT network. In 2021 IEEE 11th annual computing and communication workshop and conference (CCWC), pp. 853-859.
13. Rangelov D, Lämmel P, Brunzel L, Borgert S, Darius P, et al. (2023) Towards an integrated methodology and toolchain for machine learning-based intrusion detection in Urban IoT networks and platforms. Future Internet 15(3): 98.
14. Gao S (2022) Network Security Problems and Countermeasures of Hospital Information System after Going to the Cloud. Computational and Mathematical Methods in Medicine.
15. Wang S, Wang H, Li J, Wang H, Chaudhry J, et al. (2020) A fast CP-ABE system for cyber-physical security and privacy in mobile healthcare networks. IEEE Transactions on Industry Applications 56(4): 4467-4477.
16. Kharatyan A, Günther M, Anacker H, Japs S, Dumitrescu R, et al. (2022) Security-and Safety-Driven functional architecture development exemplified by automotive systems engineering. Procedia CIRP 109P: 586-591.
17. Nifakos S, Chandramouli K, Nikolaou CK, Papachristou P, Koch S, et al. (2021) Influence of human factors on cyber security within healthcare organizations: A systematic review. Sensors 21(15): 5119.
18. Gellert GA, Kelly SP, Hsiao AL, Herrick B, Weis D, et al. (2022) COVID-19 surge readiness: use cases demonstrating how hospitals leveraged digital identity access management for infection control and pandemic response. BMJ Health & Care Informatics 29(1): e100680.
19. Satria D, Alanda A, Erianda A, Prayama D (2018) Network security assessment using internal network penetration testing methodology. JOIV: International Journal on Informatics Visualization 2(4-2): 360-365.
20. Khan AW, Zaib S, Khan F, Tarimer I, Seo JT, et al. (2022a) Analyzing and evaluating critical cyber security challenges faced by vendor organizations in software development: SLR based approach. IEEE Access 10: 65044-65054.
21. Khan RA, Khan SU, Khan HU, Ilyas M (2022b) Systematic literature review on security risks and its practices in secure software development. ieee Access 10: 5456-5481.
22. Humayun M, Jhanjhi N, Almufareh MF, Khalil MI (2022) Security threat and vulnerability assessment and measurement in secure software development. Comput Mater Contin 71: 5039-5059.
23. DuBois E, Peper A, Albert LA (2023) Interdicting Attack Plans with Boundedly Rational Players and Multiple Attackers: An Adversarial Risk Analysis Approach. Decision Analysis 20(3): 202-219.
24. Antunes M, Silva C, Marques F (2021) An integrated cybernetic awareness strategy to assess cybersecurity attitudes and behaviours in school context. Applied Sciences 11(23): 11269.
25. Afshar M, Adelaine S, Resnik F, Mundt MP, Long J, et al. (2023) Deployment of Real-time Natural Language Processing and Deep Learning Clinical Decision Support in the Electronic Health Record: Pipeline Implementation for an Opioid Misuse Screener in Hospitalized Adults. JMIR Medical Informatics 11: e44977.
26. Coutinho B, Ferreira J, Yevseyeva I, Basto Fernandes V (2023) Integrated cybersecurity methodology and supporting tools for healthcare operational information systems. Computers & Security 129(14): 103189.
27. Lee D, Kim D, Lee C, Ahn MK, Lee W, et al. (2022) ICSTASY: An Integrated Cybersecurity Training System for Military Personnel. IEEE Access 10: 62232-62246.
28. Souppaya M, Scarfone K, Dodson D (2022) Secure software development framework (SSDF) version 1.1. NIST Special Publication 800-218.
29. Nelson CJ, Soisson ET, Li PC, Lester Coll NH, Gagne H, et al. (2022) Impact of and response to cyberattacks in radiation oncology. Advances in Radiation Oncology 7(5): 100897.
30. (2020) Cybersecurity & Infrastructure Agency (CISA) Securing network infrastructure devices.

ISSN: 2574-1241

DOI: 10.26717/BJSTR.2024.56.008926

Cheryl Ann Alexander. Biomed J Sci & Tech Res

Submission Link: https://biomedres.us/submit-manuscript.php