

ORIGINAL RESEARCH ARTICLE

Effective metrics to detect and prioritize cyber incidents in healthcare

Cheryl Ann Alexander^{1*} and Lidong Wang²¹Department of Research and Development, Institute for IT Innovation and Smart Health, Mississippi, United States of America²Institute for Systems Engineering Research, Mississippi State University, Starkville, Mississippi, United States of America

Abstract

Numerous researches have focused on metrics for detecting and prioritizing incidents or risks; however, most studies address siloed responses within a single team or department. There remains a notable gap in the literature, especially in the healthcare sector, regarding comprehensive incident and risk metrics. This gap extends beyond theoretical principles to practical applications. This paper introduces a set of metrics for detecting and prioritizing cyber incidents, risks, and attacks, with a focus on their application in healthcare. Key principles include a holistic approach to incident and risk management, and the use of both quantitative and qualitative metrics for evaluation. A case study on implementing cyber incident metrics in the Emerald Healthcare System is presented. The case study covers metrics related to incidents, planning, and strategy from risk recognition through incident resolution, as well as approaches to ensuring the readiness of an incident response plan, adopting a holistic approach to risk management, and improving healthcare cybersecurity through integrated technology design. Assessments based on artificial intelligence, machine learning, and deep learning have the potential to serve as powerful metrics. A holistic approach to risk handling helps avoid risk silos, while holistic risk management offers the best protection for hospital cyber infrastructure against malicious attacks. Protecting patient privacy is essential for any healthcare system. A robust and comprehensive approach to patient data privacy, encompassing staff training and strict access control to patient records, should be an integral part of any risk management strategy.

***Corresponding author:**Cheryl Ann Alexander
(cannalexander68@gmail.com)

Citation: Alexander CA, Wang L. Effective metrics to detect and prioritize cyber incidents in healthcare. *Artif Intell Health*. 2026;3(3):025170035. doi: 10.36922/AIH025170035

Received: April 24, 2025**1st revised:** July 17, 2025**2nd revised:** August 3, 2025**Accepted:** August 12, 2025**Published online:** October 15, 2025

Copyright: © 2025 Author(s). This is an Open-Access article distributed under the terms of the Creative Commons Attribution License, permitting distribution, and reproduction in any medium, provided the original work is properly cited.

Publisher's Note: AccScience Publishing remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Keywords: Cybersecurity; Cyber risk; Risk metrics; Incidents; Privacy; Healthcare; Artificial intelligence; Machine learning

1. Introduction

Numerous advanced technologies have been applied and adopted by various entities, such as government institutions, healthcare systems, educational institutions, and other organizations. For example, a meshfree particle computational method for cardiac image analysis was utilized to address the challenge of achieving an optimal mathematical description in cardiac image analysis. This meshfree method was validated in cardiac image segmentation and cardiac motion analysis through experimental studies.¹ Cardiac electrophysiology meshfree modeling was conducted

using the mixed collocation method, enabling rapid model generation in clinical settings along with efficient simulations.² Big data analytics, artificial intelligence (AI), machine learning (ML), deep learning (DL), and quantum cryptography have been employed in government services, the military, enterprises, marketing, manufacturing, healthcare, and other sectors.³⁻⁶ Although advanced technologies offer numerous advantages and benefits, they also introduce various risks, attacks, and threats posed by malicious actors.⁷ AI/ML/DL technologies can help detect and prioritize incidents, risks, attacks, and threats. However, cybercriminals and malicious actors can also exploit advanced technologies, such as AI/ML/DL to launch cyberattacks and pursue cybercrime objectives. Developing metrics to detect and prioritize incidents, especially in healthcare, is both necessary and significant. These metrics support the development of strategies and plans to detect incidents, risks, attacks, and threats, and to mitigate associated risks or threats.

When a Chief Information Security Officer must make decisions regarding resource allocation, conventional risk matrices often offer limited guidance. Various models exist to help cybersecurity analysts represent uncertainty, such as estimating likelihood and impacts, or developing modeling methods to determine how probabilities and effects change based on threat categories, attacker capabilities, vulnerabilities, or system features.⁸ Quantitative risk assessment provides standardized scoring but can be time-consuming to implement, while qualitative risk assessment allows for quicker decision-making.⁹ A business framework of control objectives for information and related technology has been used in a quantitative study to evaluate the maturity level of information technology (IT) services, mainly in delivery, service, and support.¹⁰

Security metrics can be used to measure the security level of system components or aspects, based on quantitative or qualitative evaluation. These metrics are generally classified into three major categories: (i) Management, (ii) operational, and (iii) technical. Additional classification approaches exist, which may be based on result types (such as qualitative or quantitative) or scope, such as devices, networks, and systems. There are four types of technical metrics:¹¹

- (i) Vulnerability metrics—measures of system vulnerabilities.
- (ii) Attack metrics—measures of the strength of sustained attacks.
- (iii) Defense metrics—measures of the strength and effort required to implement a defense mechanism within a system.
- (iv) Situation metrics—measures of the security state of a system.

The primary objective of this research is to explore effective metrics for detecting and prioritizing incidents. A major research gap exists—cyber incident silos are often the norm, while holistic risk management is insufficiently implemented. The remainder of this paper is organized as follows: Section 2 introduces metrics related to incidents, risks, and attacks; Section 3 presents risk metrics in healthcare; Section 4 provides a case study on incident metrics in healthcare, focusing on metrics used in the Emerald Healthcare System, planning and strategy from risk recognition through incident resolution, approaches to ensuring readiness of incident response plans, a holistic approach to managing risks, and improving healthcare cybersecurity through holistic technology design; and Section 5 concludes the manuscript.

2. Metrics of incidents/risks/attacks in general areas/fields

A combination of time-based metrics, volume-based metrics, and cost-related metrics should be leveraged to detect and prioritize cyber incidents effectively. Major metrics include mean time to detect (MTTD), mean time to respond/resolution (MTTR), incident severity, vulnerability management, phishing attack success rates, and others. These metrics provide insights into the efficiency of threat detection, response, and the overall effectiveness of cybersecurity practices. Table 1 presents the major metrics used to detect and prioritize cyber incidents across general areas and fields.¹²⁻¹⁶ MTTD, MTTR, and MTTC can be calculated as follows:

$$\text{MTTD} = \frac{\sum(\text{Time to detect incidents})}{\text{Number of incidents detected}} \quad (\text{I})$$

$$\text{MTTR} = \frac{\sum(\text{Time to respond to incidents})}{\text{Number of incidents responded}} \quad (\text{II})$$

$$\text{MTTC} = \frac{\sum(\text{Time to detect} + \text{Time to acknowledge} + \text{Time to resolve})}{\text{Number of incidents}} \quad (\text{III})$$

A method and a framework were proposed to derive custom dynamic cyber risk metrics. The framework and its metric goals are illustrated in Figure 1.¹⁷ Table 2 summarizes several major measurements regarding an organization's exposure, maturity levels, and attractiveness, as well as the technical and financial impacts of incidents.¹⁷ All of these impacts are expressed as quantitative measures (e.g., costs, time).

AI/ML has been both a tool for improving cybersecurity and a source of vulnerabilities. It is employed to analyze large volumes of data, detect malicious activity with high accuracy and in real time, and automate responses to threats. It can also adapt to new threats by learning from historical data and evolving attack vectors.¹⁸⁻²⁰ Figure 2

Table 1. Major metrics for the detection and prioritization of cyber incidents in general areas/fields

Metrics	Definition and features
MTTD	The average time taken to detect a security incident after it occurs
MTTR	The average time taken to respond to a detected incident
Failed login number	The number of failed login attempts, indicating suspicious activity or brute-force attacks
Intrusion attempts blocked	The number of intrusion attempts blocked by security controls
Unidentified devices on the network	The number of unidentified or unauthorized devices connected to the network, indicating potential security risks or vulnerabilities
Phishing attack success rate	The percentage of phishing attempts that successfully deceive users and lead to security incidents)
Incident severity	Categorization of incidents based on their potential impacts and criticality
Security rating	An external measure of an organization's overall security posture, used to identify areas for improvement
Mean time to contain	The average time taken to contain a security incident, covering detection and resolution
Access management metrics	Metrics tracking user access levels, privilege escalation attempts, and access controls to detect and mitigate potential insider threats
Vulnerability management metrics	Metrics tracking the number of vulnerabilities, patching cadence (how fast vulnerabilities are addressed), and vulnerability recurrence rates to evaluate the effectiveness of vulnerability management
Cost per incident	The financial impact of a security incident, including remediation costs, legal fees, and potential downtime

Abbreviations: MTTC: Mean time to contain; MTTD: Mean time to detect; MTTR: Mean time to respond.

shows the primary cyber threats that have significant impacts on critical cyber infrastructure.²¹⁻²³ An Advanced Persistent Threat is a sophisticated cyberattack.

A cybersecurity framework with procedural details was developed based on AI/ML,^{24,25} starting with the identification of cyber threats and ending with techniques for continuous learning, as illustrated in Figure 3.²⁴ Real-time monitoring is needed to detect cyber threats. The framework is designed for continuous learning, meaning it adjusts its detection techniques and algorithms as new threats emerge. The capability of the framework to effectively and accurately defend against constantly evolving cyber threats is enhanced by AI/ML-based continuous learning.



Figure 1. Metric goals in a proposed framework. Image created by the author.

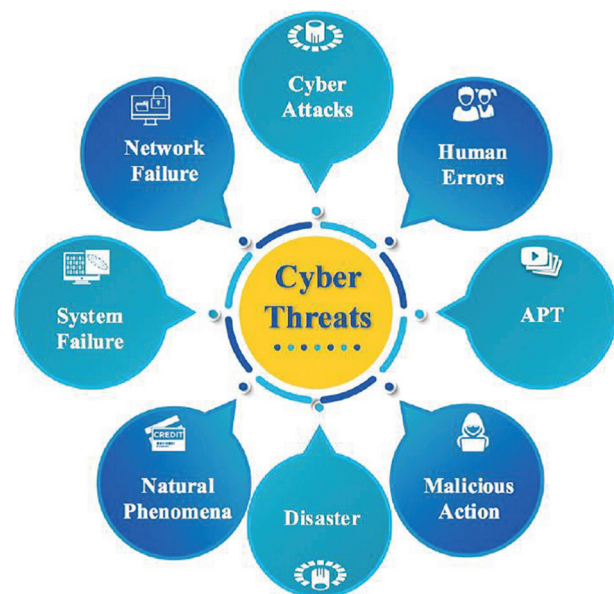


Figure 2. Primary cyber threats and impacts on critical cyber infrastructure²²

Distributed denial-of-service (DDoS) attacks can congest critical network links and paralyze the services of the Internet of Things^{26,27} and the cloud.²⁸ An AI-driven assessment framework was introduced that uses convolutional neural networks (NNs) to evaluate network status (i.e., whether a DDoS attack is occurring). This method provides a quantitative assessment of risks. Figure 4²⁹ depicts the steps of the assessment framework. In the sixth step, the sample is flattened into a 1D array, which serves as the input for the seventh step (adaptive moment estimation). Adaptive moment estimation is used to estimate the probability that the network is under

Table 2. Measurements regarding the exposure, maturity levels, and attractiveness of an organization, and the technical and financial impacts of incidents

Aspects of measurements	Measurements or measurement domains
Exposure of the organization	• Quantity of vulnerabilities • Criticality of vulnerabilities (e.g., based on the CVSS) • Criticality of affected assets • Time-based metrics: Mean time to identify, mean time to remediate
Maturity level (1 of 3) of the organization	• Cybersecurity program management: Frequency of program updates, security policy review frequency, etc. • Risk management: Frequency of risk assessment processes, control review frequency, etc. • Asset, change, and configuration management: Inventory frequency, configuration review frequency, etc. • Threat and vulnerability management
Maturity level (2 of 3) of the organization	• Identity and access management: Number of passwords complying with the password policy, access rights review frequency, etc. • Event and incident response, continuity of operations: Detection-to-decision time, number of detected events, etc.
Maturity level (3 of 3) of the organization	• Security architecture: Number of firewall rules, malware scan frequency, etc. • Third-party risk management: Number of signed agreements, specific audit frequency, etc. • Workforce management: Training frequency, training duration, number of security-certified professionals, etc.
Attractiveness of the organization	• Technological: Honeypots, number of active hybrid threats, etc. • Political and strategic: Nationality, level of competitiveness, etc. • Financial: Financial health, annual revenue, etc. • Brand and image: Reputation scores, public relations issues, etc. • Criticality of potential results: Type/number of customers, type of products or services provided
Technical impacts of incidents	• Impacts on confidentiality: Number of compromised passwords, number of customers notified of a data breach, etc. • Impacts on integrity: Number of modified files, number of modified asset configurations, etc. • Impact on availability: Downtime, number of rebooted assets, etc.
Financial impacts of incidents	• Productivity: Cost of staff idle periods, profit loss, etc. • Extortion: Cost of fees paid to adversaries or negotiators • Response and reconstruction: Cost of asset replacement and repairs, cost of incident response and recovery teams • Reputation and crisis management: Loss of clients, costs of brand repositioning, etc. • Fines, sanctions, and claims: Fines due to non-compliance, civil liability, etc.

Abbreviation: CVSS: Common vulnerability scoring system.

a DDoS attack. The higher probability between “attack” and “no attack” is output in the eighth step, after which the standard operating procedure for system recovery is executed. Finally, feedback in the form of an award or punishment for the selected action is generated in the last step to inform and improve the AI-driven assessment.

Fingerprint attacks are a problem for a biometric system. It is a challenge to identify a live fingerprint and a spoof fingerprint. However, a spoof fingerprint is a cybersecurity risk. A method was presented to help overcome the challenge based on the referential image quality metrics, the fingerprint minutiae count, and ML models that include k -nearest neighbor, support vector machine, and NN. The fingerprint dataset, LivDet CrossMatch-2015, was used. There are 502 spoof fingerprint images and 500 live fingerprint images in the dataset. Figure 5³⁰ illustrates the method and its procedures.

A risk assessment framework for an additive manufacturing (AM)/3D printing system was also proposed, as depicted in Figure 6.³¹ AM/3D printing has been widely used in the healthcare industry and has generated significant

value in this domain. The threat lifespan, defined as the active time of the indicator of compromise, is a critical factor influencing the severity of a threat. A threat analysis was performed based on the characteristics of threats to AM systems. These characteristics, shown in Figure 7,^{31,32} are important in assessing the potential impacts of threats on the AM process and its supply chains.

There are significant cybersecurity challenges in the maritime sector. Ships equipped with IT and operational technology are connected to external networks, making them vulnerable to cyberattacks. Cyber risks in the maritime sector were identified, and a qualitative risk evaluation was conducted.³³ Priorities for improving vulnerabilities were derived based on the risk evaluation and the assigned ranks for specific risk items. Table 3 presents administrative and technical security risk items along with their ranks for prioritizing vulnerability improvements.³³

3. Risk metrics in healthcare

A data breach in healthcare can lead to serious consequences. Effectively detecting and prioritizing cyber



Figure 3. A cybersecurity framework and procedural details based on artificial intelligence/machine learning. Obtained from²⁴ with permission. Copyright © 2025, IEEE.

incidents are vital to ensuring the quality of care and patient well-being. Healthcare organizations can use well-defined metrics to detect and prioritize cyber incidents, monitor and analyze these metrics regularly, and transform raw data into actionable insights. This allows for data-driven decision-making, proactive risk prevention, and continuous enhancement in patient safety. Table 4 presents metrics used for detecting and prioritizing cyber incidents in healthcare.^{12,34–39}

Although electronic health records (EHRs) offer numerous advantages, they also present significant cybersecurity challenges. A major threat to EHRs involves unauthorized access—both by internal employees and external cyber attackers—leading to breaches of patient data and privacy. Among these, external access by cyber attackers poses the highest risk to both EHRs and patient safety. A risk assessment of EHR security was conducted using a risk matrix. Table 5 shows the EHR risk matrix.⁴⁰ Various other risk measurement methods (qualitative and quantitative) have also been applied in healthcare.

4. A case study regarding incident metrics in healthcare

Emerald Healthcare System is a not-for-profit corporation dedicated to developing medical programs, healthcare

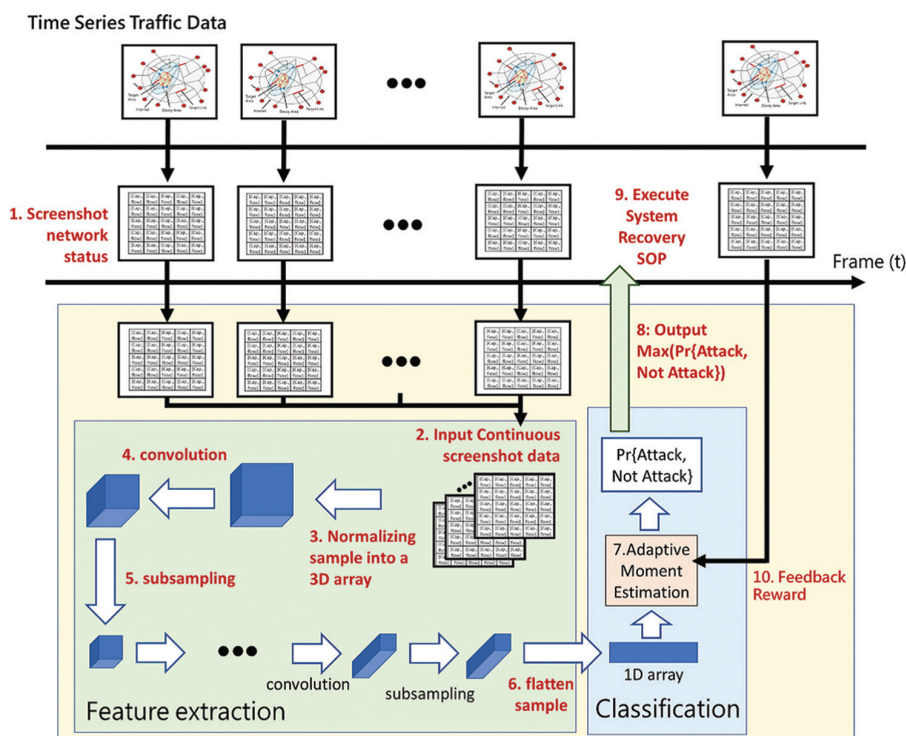


Figure 4. An artificial intelligence-driven assessment framework for evaluating network status. Adopted from²⁹ with permission. Copyright © 2021, Sage Publications. Abbreviation: SOP: Standard operating procedure.

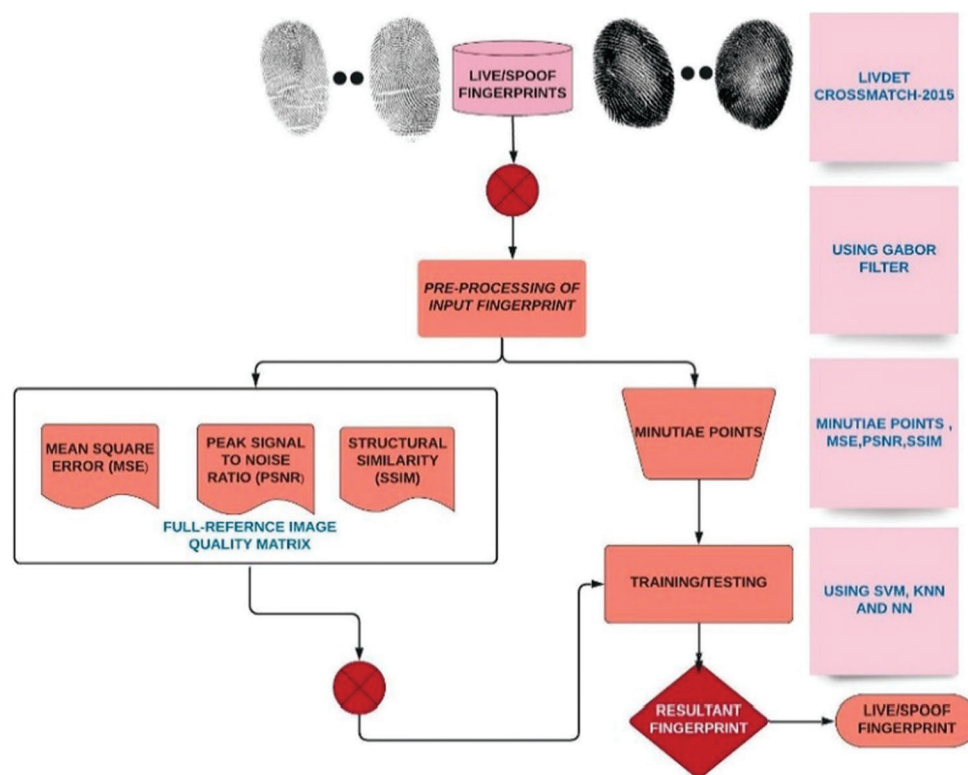


Figure 5. A method for identifying live and spoof fingerprints³⁰

Abbreviations: KNN: *k*-nearest neighbor; NN: Neural network; SVM: Support vector machine.

Table 3. Security risks and ranks for vulnerability improvement prioritization

Security areas	Evaluation items	Ranks
Administrative security	Awareness of information protection and staff training	1
	Control over the use of portable media (e.g., laptops, USB drives)	4
	Software maintenance and hardware/software upgrades	5
	Developing a contingency plan for cyberattacks	8
Technical security	Limitation and control of network ports, protocols, and services	2
	Detecting, blocking, and warning of cyberattacks through the system	3
	Wireless access control with encrypted keys	7
	Support for data backup and recovery	6

Abbreviation: USB: Universal Serial Bus

services, research, and more. The system's three hospital campuses, along with several outpatient facilities, provide a broad spectrum of care. Services are delivered by over 1,550 medical staff members and more than 10,300 employed professionals, making Emerald Healthcare System one of

the largest healthcare providers in Texas, United States of America.

4.1. Metrics of incidents in the Emerald Healthcare System

The following metrics and indicators are used in the Emerald Healthcare System to monitor and manage incidents:

- (i) Cybersecurity incidents: The severity and number of cybersecurity breaches and risks that have the potential to disrupt operations and compromise patient data privacy.
- (ii) Regulatory compliance rates:⁴¹ Reflect the organization's adherence to healthcare standards and regulations, which can influence reimbursement and legal exposure.
- (iii) Medication errors: Monitoring preventable adverse events helps reduce errors, thereby improving operational efficiency and patient safety.

Examples of specific metrics for cybersecurity incidents include: (i) Number of events in a defined time frame (e.g., daily, weekly, monthly, quarterly, or annually); (ii) average incident response time—the time from incident occurrence to its routing to the appropriate team member; (iii)

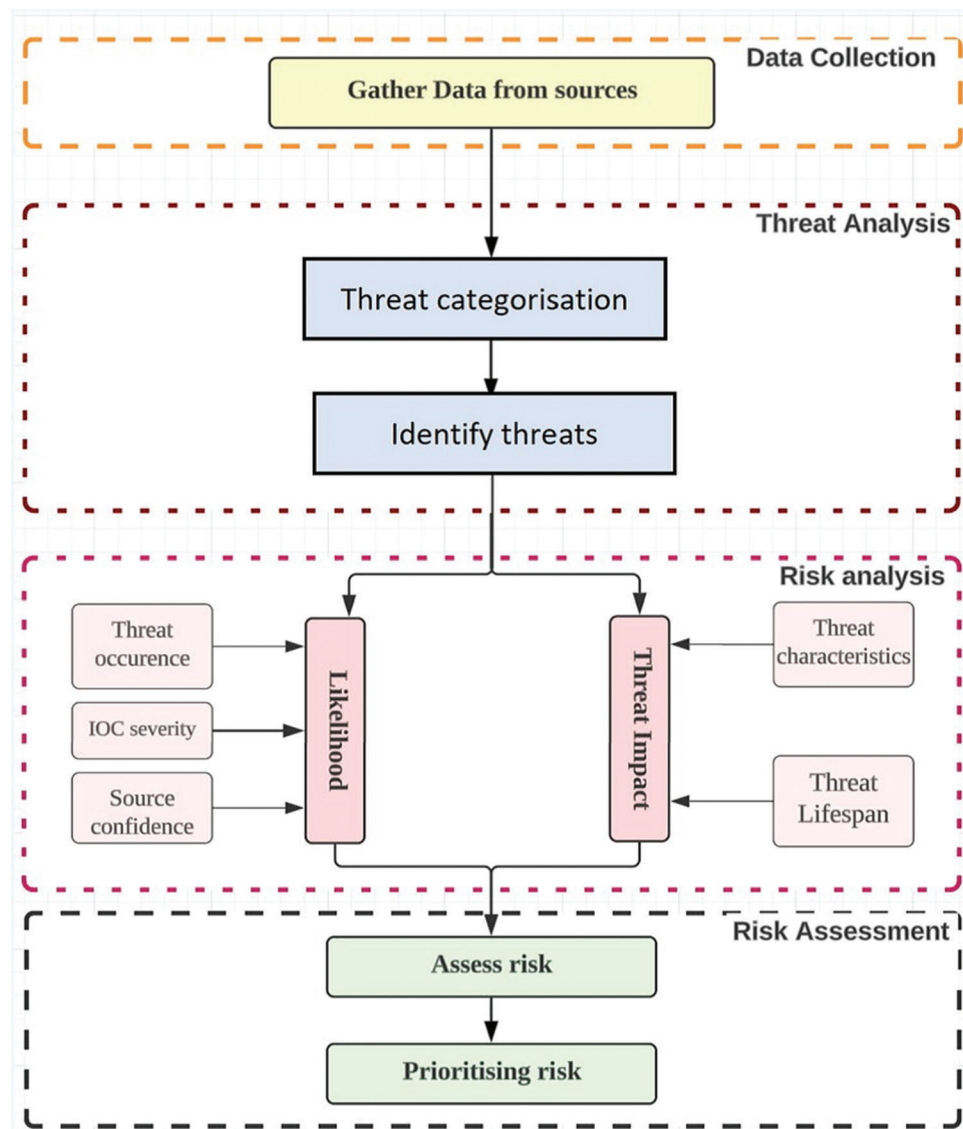


Figure 6. A risk assessment framework for an additive manufacturing/3D printing system³¹
Abbreviation: IOC: Indicator of compromise.

MTTR—the average time required to resolve an incident and return the affected system to normal operation.

4.2. Planning and strategy from risk recognition through incident resolution

A proven strategy to protect patient data includes a comprehensive incident response plan for healthcare. This can be fulfilled through the following approaches:

- (i) Internal communication: Provides precise and actionable updates regarding the nature of the event, response measures, operational disruptions, and more. Maintaining open communication channels is critical throughout the incident response process.
- (ii) Identification and containment: Early detection and prompt containment are key to minimizing the impact of a data breach.
- (iii) Eradication and recovery: These stages may include removing malware, addressing security vulnerabilities, and resetting compromised accounts.

4.3. Incident response planning framework

Establishing an incident response framework should encompass the complete lifecycle of an event. Components of the framework include: (i) Preparation; (ii) detection and analysis; (iii) containment, eradication, and recovery;

Table 4. Metrics for the detection and prioritization of cyber incidents in healthcare

Categories	Metrics and description
Incident detection and response metrics	MTTD: The average time taken to detect a security incident in healthcare from the moment it occurs
	MTTC: The average time taken to contain a security threat in healthcare and prevent its spread
	Number of security incidents: The number of security alerts in healthcare that require action from a security team
	Percentage of incidents detected by internal controls: Indicates the effectiveness of internal security measures in identifying potential threats before they cause significant damage
	Unidentified devices on internal networks: Reflects the presence of potentially malicious or unauthorized devices accessing the healthcare network
	Dwell time: Represents the duration a threat actor remains undetected within a healthcare system or network
	Mean time to recover: The average time from detecting a security incident to fully restoring all affected healthcare systems to their pre-attack state
Vulnerability and incident management metrics	Number of vulnerabilities detected: The number of known vulnerabilities identified on healthcare devices
	Vulnerability recurrence: Tracks how frequently the same vulnerabilities reappear, indicating issues with remediation or patching
	Patching cadence: Measures the frequency and consistency of applying patches to resolve vulnerabilities
	Patch compliance rate: The percentage of devices and systems in healthcare that have received the latest security patches
	Service level agreement compliance: Measures adherence to defined service levels for incident response in healthcare, often with penalties for non-compliance
	Mean time to remediate: The average time required to resolve a confirmed vulnerability
	Customer satisfaction score: Feedback from end users on their experience with the incident management process, highlighting areas for improvement
Other significant metrics	Intrusion attempts: The number of attempted breaches or unauthorized access in healthcare
	Phishing click rate: The percentage of users who click on malicious links in phishing emails
	Average vendor security rating: Reflects the overall cybersecurity posture of third-party vendors. Monitoring this helps manage risks from external partners
	Data breach costs: The financial impact of healthcare breaches, including detection, notification, response, lost business, and regulatory fines
	Medical device security adoption: Indicates the extent to which security measures (e.g., real-time monitoring) have been implemented for medical devices
	Compliance success rates: Measures adherence to healthcare regulations, such as HIPAA

Abbreviations: HIPAA: Health insurance portability and accountability act; MTTC: Mean time to contain; MTTD: Mean time to detect.

Table 5. A risk matrix of EHR

Risks	Probabilities	Impacts	Description
Cyberattacks on EHR	High	High	Targeting EHR through outdated technologies and security loopholes can lead to major patient data breaches
Insider threats	Medium	High	Misuse or mishandling of sensitive data by individuals with access to EHR can result in unauthorized disclosure or manipulation of information
Loss/theft of devices	Medium	Medium	Loss or theft of devices used by healthcare staff to access EHR may result in unauthorized access to sensitive data
Technology failures	Medium	High	Failures in the technologies supporting EHR systems can lead to data corruption or loss, impacting healthcare operations and patient care
Legal/regulatory non-compliance	High	High	Failure to comply with healthcare regulations and data protection laws can lead to fines, legal actions, and loss of trust among patients and partners
Third-party data sharing	Medium	Medium	Unauthorized or unintended data sharing with third parties may result in privacy breaches and diminished patient trust

Abbreviation: EHR: Electronic health record.

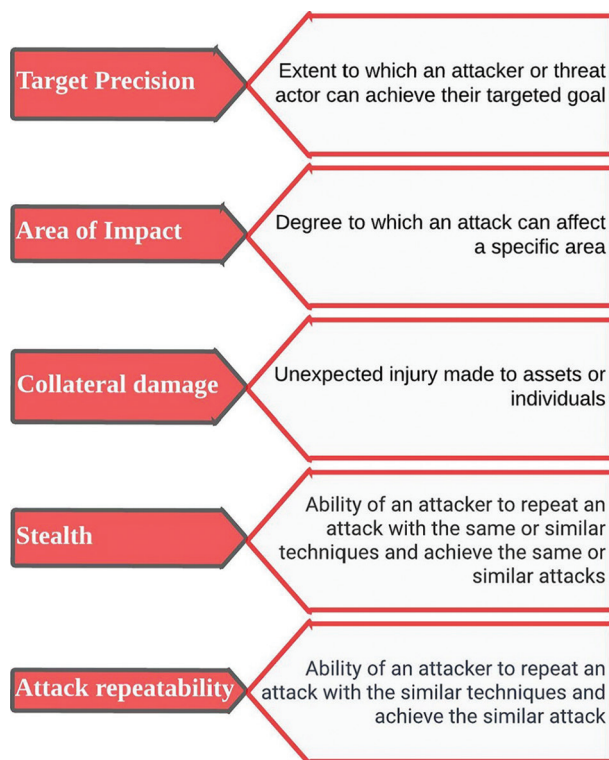


Figure 7. Features of threats in additive manufacturing/3D printing³¹

and (iv) post-incident activities. Understanding common occurrences and integrating them into IT team policies and procedures is critical for preparing against future attacks. Some common occurrences include: (i) Improper or inappropriate usage; (ii) unauthorized access; (iii) denial of service; (iv) malicious code; (v) suspected personal health information breach—any event involving personal health information should be reported, even if only suspected; and (vi) suspected loss of sensitive data.

In the event of an incident, response efforts should not be siloed within a single team or department. Establishing a cross-functional incident response team ensures a multi-faceted, integrated approach to incident management. It is essential that IT security teams understand the core components of a viable incident response plan. These components include preparation, detection, triage, incident analysis, containment, eradication, recovery, remediation, post-incident activity and review, and supplier facility and/or service tests. The primary triage stage helps determine the severity and response level of an incident and aids in setting priorities for subsequent response steps.

4.4. Holistic risk management and integrated risk perspectives

To avoid “risk silos,” holistic risk management (also known as integrated risk management)^{18,42} emphasizes the need to

address the fragmented nature of functions and processes that often focus on limited aspects of risks, typically divided by business lines or departments. Several components constitute a holistic approach to risk management, including policy management and management framework; organizational structuring to understand and address risk across silos; and an investigation and measurement framework, including relevant metrics.

In the Emerald Healthcare System, clinical and administrative systems, processes, and reports are utilized to detect, assess, monitor, mitigate, and prevent risks. Risk management in the healthcare system encompasses several critical elements, such as risk identification, risk quantification and prioritization, compliance reporting, and the use of models for incident analysis to understand the causes and effects of medical errors. These models include failure mode and effects analysis, root cause analysis, and others.

4.5. Holistic technology in healthcare cybersecurity

A holistic approach to cybersecurity offers the most effective protection for hospital cyber infrastructure against malicious attacks. It is essential to design a comprehensive risk assessment framework in the context of population health management. The Emerald Healthcare System uses several risk assessment models, incorporating modules that include historical health service utilization (e.g., emergency department visits, hospital admissions, urgent care visits, and preventive screening), health risk evaluations, and various forecasting mechanisms to project future utilization.

5. Conclusion

Security metrics can be classified into three categories: (i) Management, (ii) operational, and (iii) technical. These metrics can be either qualitative or quantitative. AI/ML-driven assessments have the potential to serve as powerful metrics. The risk matrix can be used in the risk assessment of the security of EHR. Major metrics and indicators for incidents used in the Emerald Healthcare System include cybersecurity incidents, regulatory compliance rates, and medication errors. A holistic approach to handling risks helps avoid risk silos. Holistic risk management is most effective in protecting hospital cyber infrastructure from malicious attacks. Protecting patient privacy is critical for any healthcare system. A rigorous and holistic approach to patient data privacy, which includes staff training on patient privacy and its potential vulnerability following a cyberattack. Patient privacy and strict rules for accessing a patient’s chart should be incorporated into any risk management plan.

Acknowledgments

The authors would like to thank Technology and Healthcare Solutions, United States of America, for their assistance and support.

Funding

None.

Conflict of interest

The authors declare that they have no competing interests.

Author contributions

Conceptualization: Cheryl Ann Alexander

Formal analysis: All authors

Investigation: Cheryl Ann Alexander

Methodology: All authors

Writing – original draft: Cheryl Ann Alexander

Writing – review & editing: All authors

Ethics approval and consent to participate

Not applicable.

Consent for publication

Not applicable.

Availability of data

Data from this study are available from the corresponding author upon reasonable request.

References

1. Zhang H, Gao Z, Xu L, *et al.* A meshfree representation for cardiac medical image computing. *IEEE J Transl Eng Health Med.* 2018;6:1-12.
doi: 10.1109/JTEHM.2018.2795022
2. Mountris KA, Pueyo E. Cardiac electrophysiology meshfree modeling through the mixed collocation method. *Appl Sci.* 2023;13(20):11460.
doi: 10.3390/app132011460
3. Abisoye A, Akerele JI, Odio PE, Collins A, Babatunde GO, Mustapha SD. Using AI and machine learning to predict and mitigate cybersecurity risks in critical infrastructure. *Int J Eng Res Dev.* 2025;21(2):205-224.
4. Jhessim E, Anku V. Quantum computing for cybersecurity in healthcare systems: A multi-modal approach. *Int J Sci Res Arch.* 2025;14(1):612-622.
doi: 10.30574/ijrsra.2025.14.1.0127
5. Maharaj AV, Arbour D, Lee D, *et al.* Evaluation and Incident Prevention in an Enterprise AI Assistant. In: *Proceedings of the AAAI Conference on Artificial Intelligence.* Association for the Advancement of Artificial Intelligence. 2025;39(28):28931-28937.
doi: 10.1609/aaai.v39i28.35161
6. Sodhro AH, Mughal MI, Iqbal MJ. 5G beyond for healthcare: Leveraging AI/ML and diverse datasets for cybersecurity. In: *International Workshop on Secure and Resilient Digital Transformation of Healthcare.* Cham: Springer Nature Switzerland; 2024:45-66.
doi: 10.1007/978-3-031-85558-0_3
7. Islam E, Rudolph C, Oliver G. Managing cyber harm: A survey of challenges, practices, and opportunities. *Inform Secur J Glob Perspect.* 2025;34:424-454.
doi: 10.1080/19393555.2025.2484348
8. Hubbard DW, Seiersen R, Geer DE, McClure S. *How to Measure Anything in Cybersecurity Risk.* United States: Wiley; 2016.
9. Harry C, Sivan-Sevilla I, McDermott M. Measuring the size and severity of the integrated cyber attack surface across US county governments. *J Cybersecur.* 2025;11(1):tyae032.
doi: 10.1093/cybsec/tyae032
10. Amali LN, Katili MR, Suhada S, Hadjaratie L. The measurement of maturity level of information technology service based on COBIT 5 framework. *Telkomnika (Telecomm Comput Electron Control).* 2020;18(1):133-139.
doi: 10.12928/telkomnika.v18i1.10582
11. Gori G, Rinieri L, Al Sadi A, Melis A, Callegati F, Prandini M. Graph4: A security monitoring architecture based on data plane anomaly detection metrics calculated over attack graphs. *Future Internet.* 2023;15(11):368.
doi: 10.3390/fi15110368
12. Ahmed M, Pathan AS. False data injection attack (FDIA): An overview and new metrics for fair evaluation of its countermeasure. *Complex Adapt Syst Model.* 2020;8:1-14.
doi: 10.1186/s40294-020-00070-w
13. Algarni AM, Thayananthan V, Malaiya YK. Quantitative assessment of cybersecurity risks for mitigating data breaches in business systems. *Appl Sci.* 2021;11(8):3678.
doi: 10.3390/app11083678
14. Iganibo I, Albanese M, Mosko M, Bier E, Brito AE. An attack volume metric. *Secur Privacy.* 2023;6(4):e298.
doi: 10.1002/spy2.298
15. Maulita I, Hayadi BH. Financial loss estimation in cybersecurity incidents: A data mining approach using decision tree and linear regression models. *J Cyber Law.* 2025;1(2):161-174.
doi: 10.63913/jcl.v1i2.9
16. Ramli A, Darus MY, Mohd Yusoff Y, Azni B. Integrated cybersecurity framework for enhanced threat detection

- and incident response in the digital era. *Malays J Comput.* 2025;10(1):2099-2116.
doi: 10.24191/mjoc.v10i1.4520
17. Calvo M, Beltrán M. Applying the Goal, Question, Metric method to derive tailored dynamic cyber risk metrics. *Inform Comput Secur.* 2024;32(2):133-158.
doi: 10.1108/ICS-03-2023-0043
18. Babatunde GO, Mustapha SD, Ike CC, Alabi AA. A holistic cyber risk assessment model to identify and mitigate threats in us and Canadian enterprises. *Int J Multidiscip Res Growth Eval.* 2025;6(1):773-787.
doi: 10.54660/IJMRGE.2025.6.1.773-787
19. Chatziamanetoglou D, Rantos K. Weighted quality criteria for cyber threat intelligence: Assessment and prioritisation in the MISP data model. *Int J Inform Secur.* 2025;24(4):1-35.
doi: 10.1007/s10207-025-01080-6
20. Jones RK. AI automated incident response and threat mitigation using AI. In *Revolutionizing Cybersecurity with Deep Learning and Large Language Models*. United States: IGI Global Scientific Publishing; 2025:201-236.
doi: 10.4018/979-8-3373-3296-3.ch007
21. Aljumaiah O, Jiang W, Addula SR, Almaiah MA. Analyzing cybersecurity risks and threats in IT infrastructure based on NIST framework. *J Cyber Secur Risk Audit.* 2025;2025(2):12-26.
doi: 10.63180/jcsra.thestap.2025.2.2
22. Djenna A, Harous S, Saidouni DE. Internet of things meet internet of threats: New concern cyber security issues of critical cyber infrastructure. *Appl Sci.* 2021;11(10):4580.
doi: 10.3390/app11104580
23. Ogunsanya VA, Adesokan A, Eleweke I, Obu AU, Afolabi R, Abbas R. Cybersecurity incidents on digital infrastructure and industrial networks. *J Computat Anal Appl.* 2025;34(3):85-106.
24. Bonagiri K, Krishnamoorthy P, Keerthiga V, Kirubakaran D, David R, Nanchariaiah B. Cybersecurity with machine learning: Implementing AI Algorithms for Intrusion Prevention, Advanced Data Protection, and Real-Time Threat Analysis. In: *2025 International Conference on Computational, Communication and Information Technology (ICCCIT), Indore, India; 2025.* p. 292-298.
doi: 10.1109/ICCCIT62592.2025.10928115
25. Kalpinagarajarao GK, Gopalan R. AI-enhanced oracle platforms: A new era of predictive healthcare analytics and cybersecurity. *Int J Multidiscip Res Growth Eval.* 2025;6(1):1823-1830.
doi: 10.54660/IJMRGE.2025.6.1-1823-1830
26. ElSayed Z, Abdelgawad A, Elsayed N. Cybersecurity and Frequent Cyber Attacks on IoT Devices in Healthcare: Issues and Solutions. *arXiv*. Preprint posted online 2025.
doi: 10.48550/arXiv.2501.11250
27. Ozcelik MM, Kok I, Ozdemir S. A survey on internet of medical things (IoMT): Enabling technologies, security and explainability issues, challenges, and future directions. *Expert Syst.* 2025;42(5):e70010.
doi: 10.1111/exsy.70010
28. Tiwo OJ, Adesokan-Imran TO, Babarinde DC, Salami IA, Onyenaucheya OS, Olaniyi OO. Improving patient data privacy and authentication protocols against AI-powered phishing attacks in telemedicine. *Asian J Res Comput Sci.* 2025;18(4):93-114.
doi: 10.9734/ajrcos/2025/v18i4610
29. Chen YH, Chang A, Huang C. Using learning time as metrics: An artificial intelligence driven risk assess framework to evaluate DDoS cyber attack. *J Intell Fuzzy Syst.* 2021;40(4):7691-7699.
doi: 10.3233/JIFS-189589
30. Verma A, Gupta A, Akbar M, Yadav AK, Yadav D. Fingerprint Presentation Attack Detection using Referential Quality Metrics and Minutiae Count. *Research Square*. Preprint posted online September 21, 2021.
doi: 10.21203/rs.3.rs-792415/v1
31. Kumar M, Epiphanou G, Maple C. Comprehensive threat analysis in additive manufacturing supply chain: A hybrid qualitative and quantitative risk assessment framework. *Prod Eng.* 2024;18:955-973.
doi: 10.1007/s11740-024-01283-1
32. Yampolskiy M, Skjellum A, Kretzschmar M, Overfelt RA, Sloan KR, Yasinsac A. Using 3D printers as weapons. *Int J Crit Infrastruct Protect.* 2016;14:58-71.
doi: 10.1016/j.ijcip.2015.12.004
33. Yoo Y, Park HS. Qualitative risk assessment of cybersecurity and development of vulnerability enhancement plans in consideration of digitalized ship. *J Mar Sci Eng.* 2021;9(6):565.
doi: 10.3390/jmse9060565
34. Balogun AY. Strengthening compliance with data privacy regulations in US healthcare cybersecurity. *Asian J Res Comput Sci.* 2025;18(1):154-173.
doi: 10.9734/ajrcos/2025/v18i1555
35. Cornejo GM. Assessing cybersecurity dynamics: A comparative analysis of data breaches in urban and rural hospitals in the United States. *Secur J.* 2025;38(1):25.
doi: 10.1057/s41284-025-00475-3
36. Fleming P, O'Donoghue C, Almirall-Sanchez A, et al. Metrics and indicators used to assess health system

- resilience in response to shocks to health systems in high income countries-A systematic review. *Health Policy*. 2022;126(12):1195-1205.
doi: 10.1016/j.healthpol.2022.10.001
37. Kurniawan A, Darus MY, Mohd Ariffin MA, Muliono Y, Pardomuan CR. Automation of quantifying security risk level on injection attacks based on common vulnerability scoring system metric. *Pertanika J Sci Technol*. 2023;31(3): 1245-1265.
doi: 10.47836/pjst.31.3.07
 38. Tiwo OJ, Adesokan-Imran TO, Babarinde DC, Oyekunle SM, Olutimehin AT, Olaniyi OO. Advancing security in cloud-based patient information systems with quantum-resistant encryption for healthcare data. *Asian J Res Comput Sci*. 2025;18(4):187-208.
doi: 10.9734/ajrcos/2025/v18i4615
 39. Verulava T, Jorbenadze R, Ghonghadze A, Dangadze B. Introducing critical incident reporting system as an indicator of quality healthcare in Georgia. *Hosp Top*. 2022;100(2): 77-84.
doi: 10.1080/00185868.2021.1926384
 40. Alarfaj KA, Rahman MH. The risk assessment of the security of electronic health records using risk matrix. *Appl Sci*. 2024;14(13):5785.
doi: 10.3390/app14135785
 41. Covarrubias JZ. Effective communication as a pillar of cybersecurity: Managing incidents and crises in the digital era. *J Risk Anal Crisis Response*. 2025;15(2):239-272.
doi: 10.54560/jracr.v15i2.564
 42. Janani K. The Human-Machine Identity Blur: A Unified Framework for Cybersecurity Risk Management in 2025. *arXiv*. Preprint posted online 2025.
doi: 10.48550/arXiv.2503.18255