Asia Pacific Academy of Science Pte. Ltd.

*Computer and Telecommunication Engineering* 2025, 3(1), 3118.
https://doi.org/10.54517/cte3118

Article

# Cyber risk management: Theories, frameworks, models, and practices

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

[1] Institute for IT Innovation and Smart Health, Vicksburg, MS 39180, USA
[2] Institute for Systems Engineering Research, Mississippi State University, Vicksburg, MS 39180, USA
*** Corresponding author:** Cheryl Ann Alexander, cannalexander68@gmail.com

**CITATION**

Alexander CA, Wang L. Cyber risk management: Theories, frameworks, models, and practices. Computer and Telecommunication Engineering. 2025; 3(1): 3118. https://doi.org/10.54517/cte3118

**ARTICLE INFO**

Received: 2 December 2024
Accepted: 7 March 2025
Available online: 14 March 2025

**Abstract:** Cyber risks have been a major concern even if more advanced technologies have been used to deter or mitigate cyberattacks. Much research has been conducted in the areas of cyber risks and cybersecurity. Handling cyber risks needs the specific support of the theories, frameworks, and models of cyber risk management. This paper introduces theories for managing cyber risks, frameworks for handling cyber risks, models for managing cyber risks, and cyber risk management and practices. Cyber risk management and threat intelligence provide their technologies and standards. Healthcare organizations must provide robust cybersecurity procedures. Big data analytics, artificial intelligence (AI)/machine learning (ML)/deep learning (DL), etc., have thus far offered significant advances in cybersecurity for healthcare agencies. This paper will also present a case study of managing cyber risks, which will demonstrate how successful these theories, frameworks, models, and practices have been in healthcare. This paper is not a more in-depth qualitative or quantitative analysis but focuses on identifying, justifying, and describing certain key issues regarding cyber risks.

**Keywords:** cybersecurity; cyber risks; deep learning (DL); game theoretic approach (GTA); goal and effect (G&E) model; threat intelligence; healthcare

## 1. Introduction

Risk identification is the first and critical step of the risk management process. With the progress of a program, more information regarding the program will be obtained, and the risk statement will be updated. New risks will be detected as the project progresses. Therefore, risk identification is an iterative process [1]. Security and privacy controls often involve policy, oversight, supervision, automated mechanisms, and manual processes. There are three approaches to control implementation: 1) common (inheritable) control, 2) system-specific control, and 3) hybrid control. A common control is often inherited from multiple systems or programs and many sources. A system-specific control can bring risks if it is not interoperable with common controls. A hybrid control can be used if one part of the control is system-specific and the other part is common (inheritable) [2].

The investigation of the internal dynamics of IT risk organizations contributed to a theory of risk management. Four approaches (proactive, reactive, adaptive, and reflexive) to risk management were presented [3]. A toolkit for cyber and privacy risk management was proposed, and it is called AMBIENT (Automated Cyber and Privacy Risk Management Toolkit). The toolkit consists of three main modules: cybersecurity risk assessment, privacy risk assessment, and risk mitigation [4].

Reducing and mitigating cyber risks is very important for companies. There will be negative impacts on companies when cyberattacks are successful. The value of companies that are targeted by cyber risks decreases with an adverse cyberattack event. Successful cyberattacks with personal financial information loss provide adverse information regarding cyber risks to targeted companies, their stakeholders, and their competitors [5]. In addition, such situations harm the value of insurance companies that cover the damage due to cyberattacks [6].

The primary purpose of the research in this paper is to deal with theories, frameworks, models, and practices of cyber risk management. It is not a more in-depth qualitative or quantitative analysis but focuses on identifying, justifying, and describing certain key issues regarding cyber risks. The remainder of this paper will be organized as follows: The second section introduces theories for managing cyber risks; the third section presents frameworks for handling cyber risks; the fourth section introduces models for managing cyber risks; the fifth section presents cyber risk management and practices; the sixth section is a case study of managing cyber risks; and the seventh section is the conclusion.

## 2. Theories for managing cyber risks

Deep learning and extreme value theory have been used in modeling and predicting multivariate cyber risks. It is easy to handle high-dimensional cyber risks due to deep learning while using the extreme value theory to model and predict high quantiles [7]. The Internet of Things (IoT) has been used in industries (such as smart factories), healthcare, transportation, smart cities, etc. There are many benefits of IoT; for example, it helps hospitals monitor patients and medical devices. However, it also brings security risks and privacy problems [8]. There are various IoT risks, such as technical IoT risks, security IoT risks, privacy IoT risks, and ethical IoT risks. IoT risk assessment theories include Game-theoretic Computing, Cyber Security Games, Failure Mode Effects Analysis (FMEA), Fuzzy Set Theory (FST), and Dempster Shafer Theory (DST) [9].

Game-theoretic Computing has been utilized to quantitatively assess risks in cybersecurity and other areas; however, it is difficult for the theory to handle uncertainty and human factors. Cyber Security Game is employed to quantitatively differentiate digital security hazards, but it is in a simplified manner, without accurately reflecting the complexity of cyber risks. The Game Theoretic Approach (GTA) helps manage cyber risks. Game theory provides a mathematical framework to model the cooperation or conflicts between two or more individuals [9,10].

FMEA has been utilized in differentiating possible failure modes, circumstances, and areas with problems. It can examine the following elements regarding data security: infrastructure, communication security, security management, access to frameworks and data, and improvement of secure data systems. The disadvantages of FMEA are time-consuming, ineffective in handling a complicated system with multiple failures, etc. [9]. The FMEA method was changed by using game theory to evaluate the probability of risks in cyber-physical security. The method employs game theory to model the rivalry between a system and an attacker as a game, perform analysis, and find the probability of the attacker’s behavior [11].

FST is used to improve decision-making in case of ambiguity. The potential of FST, IoT, and blockchain in the development of the energy infrastructure was studied. A major disadvantage of FST lies in the complexity and difficulty of testing and validating a fuzzy system [12]. DST can integrate various types of data, which makes it a useful tool for information fusion. It has been used in risk assessment. It can handle uncertain information and improve the accuracy of decision-making in emergency management. In healthcare, it can fuse various diagnostic data, resolve conflicts between various tests, and improve diagnostic accuracy. It has limitations such as requiring all evidence to be independent and complicated computation with large data sets [13].

## 3. Frameworks for handling cyber risks

**Table 1** shows the classification of cyberattacks. There have been many frameworks for handling risks and cybersecurity. Both the National Institute of Standards and Technology (NIST) and the International Organization for Standardization (ISO) have developed frameworks for risk management and cybersecurity. Quantitative, qualitative, or combined assessments are employed in risk assessment. NIST addresses effective and documented processes regarding risk assessment and management, and software development and automation tools are required for its easy use. ISO defines the standardization of risk assessment and management, providing guidelines but not offering mechanisms to ensure compliance. The SWOT analyses of NIST and ISO in risk assessment are shown in **Tables 2** and **3**, respectively [14].

**Table 1.** Categories and subtypes of cyberattacks [15].

| Attack categories | Subtypes | Categories of triads |
|---|---|---|
| Access attack | Password attack, port redirection attack, trust exploitation attack | Confidentiality |
| Malware attack | Worm, Trojan horse, bio malware, drive-by attack, ransomware attack | Confidentiality<br>Integrity<br>Availability |
| Phishing attack | Spear phishing attack, whale phishing attack | Confidentiality<br>Integrity |
| Cryptographic attack | Linear crypt attack, differential crypt analysis, replay attack, side channel attack, attention-based LSTM encoder-decoder | Confidentiality<br>Integrity |
| Reconnaissance attack | Ping sweeps attack, port scanning attack, packet sniffer attack | Confidentiality |
| Web attack | Denial-of-service (DoS) attack, cross-site scripting, SQL injection, session hijacking | Confidentiality<br>Integrity<br>Availability |
| Passive attack | Traffic analysis attack, message content release | Confidentiality<br>Availability |
| Active attack | Replay attack, message modification attack, impersonation attack, Masquerade attack | Confidentiality<br>Integrity<br>Availability |
| Quantum attack | Individual attack, collective attack, coherent attack, intercept resend attack, time-shift attack, detector blinding attack, photon number splitting attack | Confidentiality<br>Availability |

**Table 2.** The SWOT analysis of NIST in risk assessment [14].

| | |
|---|---|
| **Strengths**<br>Standardization, being extensive, large size, and extensive scope | **Weaknesses**<br>Lack of automation tools and support |
| **Opportunities**<br>Tool supporting | **Threats (risks)**<br>Complexity, being time-consuming in documenting/updates |

**Table 3.** The SWOT analysis of ISO in risk assessment [14].

| | |
|---|---|
| **Strengths**<br>Standardization, covering risk evaluation and risk management | **Weaknesses**<br>Being non-compliant or unreachable consensus, requiring a level of compulsory compliance |
| **Opportunities**<br>Extension, cyber risk evaluation | **Threats (risks)**<br>Fairness/completeness, depending on voluntary compliance & consensus |

In addition to NIST and ISO frameworks, five privacy framework functions can be used to handle privacy risks, including Identify-P, Govern-P, Control-P, Communicate-P, and Protect-P. Additional functions (Detect, Respond, and Recover) from the cybersecurity framework can be used to facilitate the management of risks regarding security-related privacy [16]. These functions and categories are shown in **Table 4**.

**Table 4.** Privacy framework functions and categories [16].

| Functions | Categories |
|---|---|
| Identify-P | Business environment<br>Inventory & mapping<br>Risk management of the data processing ecosystem<br>Risk assessment |
| Govern-P | Policies, processes, & procedures of governance<br>Strategy for risk management<br>Monitoring & review<br>Awareness & training |
| Control-P | Policies, processes, & procedures of data processing<br>Management of data processing<br>Disassociated processing |
| Communicate-P | Policies, processes, & procedures of communication<br>Awareness of data processing |
| Protect-P | Data protection policies, processes, & procedures<br>Data security<br>Protective technologies<br>Identity management, authentication, & access control<br>Maintenance |
| Detect | Continuous security monitoring<br>Detection processes<br>Anomalies & events |
| Respond | Response planning<br>Communication<br>Analysis<br>Mitigation<br>Improvement |
| Recover | Recovery planning<br>Communication<br>Improvement |

## 4. Models for managing cyber risks

Models for the management of cyber risks include GTA, Bayesian Network, Operationally Critical Threat and Vulnerability Evaluation, Central Computer and Telecommunications Agency Risk Analysis and Management, etc. GTA-based models demonstrate performance and cost advantages over other models in managing cyber risks. GTA-based models include Fault Tree Analysis, Chain-of-Events, ISO/IEC 27002, COBIT 5, and System-Theoretic Accident Models and Processes. These models have been evolving, and improvements are still needed [10].

For a qualitative assessment on an ordinal scale of the severity of cyberattacks from experts, it is ordinary to use ordered response models. How cumulative link models could be used to evaluate cyber risks was presented. These kinds of models only need ordinal data for a response variable. The severity of a cyberattack is regarded as a function of explanatory variables that describe the features of the cyberattack [17].

A prediction model of cyber risks was presented using common vulnerabilities and exposures (CVE). This method eradicates the bias of expert opinions in the prediction of cyber risks. **Table 5** lists the top ten cybersecurity topic groups with the most frequencies among the CVE in the National Vulnerabilities Database (NVD) for all the years [18], which shows that Transport Layer Security has the most occurrences. **Table 6** lists the top ten cybersecurity topic groups that are the riskiest among the CVEs in the NVD for all the years, which shows that Transport Layer Security is the highest risk.

**Table 5.** Top ten cybersecurity topic groups with the most frequencies among the CVEs in the NVD [18].

| Ranks | CAV topics with the most frequencies |
|---|---|
| 1 | Security of the transport layer |
| 2 | Cross-site scripting |
| 3 | Injection of SQL |
| 4 | List of port numbers of TCP (Transmission Control Protocol) & UDP (User Datagram Protocol) |
| 5 | Adobe Flash Player |
| 6 | History of IOS version |
| 7 | History of Firefox version |
| 8 | Cross-site request forgery |
| 9 | Cookies of HTTP |
| 10 | JavaScript |

**Table 6.** Top ten cybersecurity topic groups that are riskiest among the CVEs in the NVD [18].

| Ranks | Riskiest CAV topics |
|---|---|
| 1 | Transport layer security |
| 2 | Adobe Flash Player |
| 3 | SQL injection |
| 4 | List of port numbers of TCP & UDP |
| 5 | Cross-site scripting |
| 6 | History of IOS version |
| 7 | History of Firefox version |
| 8 | Cross-site request forgery |
| 9 | Code injection |
| 10 | JavaScript |

Researchers Ahn et al. proposed a hierarchical multi-stage cyberattack scenario modeling method based on the goal and effect (G&E) model [19]. Different goals of attacks and their damage effects can be represented. **Table 7** lists the description and features or attributes of G&E models.

**Table 7.** Description and attributes of G&E models [19].

| Names | Description | Attributes |
|---|---|---|
| Social engineering | Get a preliminary foothold on a network | CVE (common vulnerabilities and exposures) list, open probability of file, included malicious behaviors or actions |
| Reconnaissance | Get the knowledge of the internal network & system | Target device, range of scan, start time, duration, inter-arrival time, size of packet |
| Escalation of privileges | Get permission on a network or system | CVE list, type of privilege, probability of getting the privilege |
| Forgery | Damage the integrity | Target file, CVE list, probability of forgery, including malicious behaviors or actions |
| DoS (denial of service) | Flooding attacks | Target device, type of flooding, start time, duration, inter-arrival time, size of packet |
| Command & control | An attacker communicates with a system under its control within a target network & sends controlled code on a remote or local system | C&C server, interval, included malicious behaviors or actions |
| Exfiltration | Exfiltrate information, particularly delete information & documents from a targeted network | CVE list, probability of info-leak, the interval of the leak, start time, duration, size of the packet |
| Destroying devices | Destruction of a system | Targeted devices, start time, duration |
| Spreading | Attacks of worm propagation | CVE list, target mode, interval, probability of infection, including malicious behaviors or actions |
| Consumption of resources | Consumption of CPU/memory resources | Start time, duration, usage |

## 5. Cyber risk management and practices

A significant part of the operational risk management of an enterprise is performing an inventory of risks [20]. It is impossible to eliminate risks. Many frameworks are utilized for risk management. NIST has provided various frameworks regarding security and privacy controls. **Figure 1** shows three pillars of risk management [21]. **Table 8** shows a risk management framework (RMF) and seven steps that are necessary for the effective implementation of the RMF.

Risk Control
& Reduction
Risk
Analysis
Risk
Evaluation

**Figure 1.** Pillars of risk management.

**Table 8.** Risk management framework (RMF) and steps [21].

| **Steps** | **Description** |
|---|---|
| Prepare | Prepare to ensure that an organization is ready to execute the following six main steps. |
| Categorize | Categorize the system & information according to the analysis of the impact of loss. |
| Select | Select an initial set of controls for the system & tailor the controls as needed to decrease risks to a suitable level according to a risk evaluation. |
| Implement | Perform controls & describe how controls are used. |
| Assess | Evaluate controls & decide whether controls are executed properly, operating as intended, & leading to favorite outcomes according to the requirements of security & privacy. |
| Authorize | Authorize common controls or the system according to a decision that the risk is acceptable. |
| Monitor | Monitor the system & related controls |

**Figure 2** [14] shows risk management within a trust risk awareness context. Trust and risk are coupled with each other. A system or item with a low level of trust is regarded as a high level of risk and vice versa. The risk evaluation can follow one of the following methods: qualitative, quantitative, or combined.

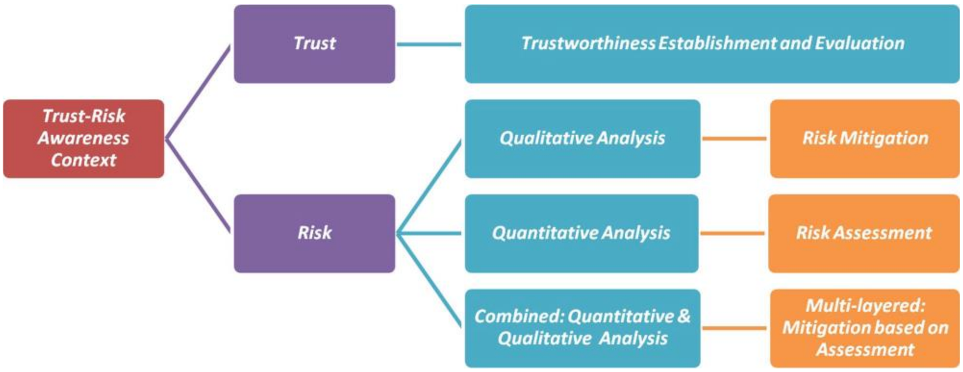
Trust-Risk Awareness Context
Trust
Trustworthiness Establishment and Evaluation
Risk
Qualitative Analysis
Risk Mitigation
Quantitative Analysis
Risk Assessment
Combined: Quantitative & Qualitative Analysis
Multi-layered: Mitigation based on Assessment

**Figure 2.** The trust-risk awareness context.

Threat intelligence and assessment is a continuous and dynamic process. A risk management framework was proposed, which is shown in **Figure 3** [22]. In the framework, a process of active threat intelligence unceasingly produces intelligence information on cyber threats and supplies it into the process of risk management.

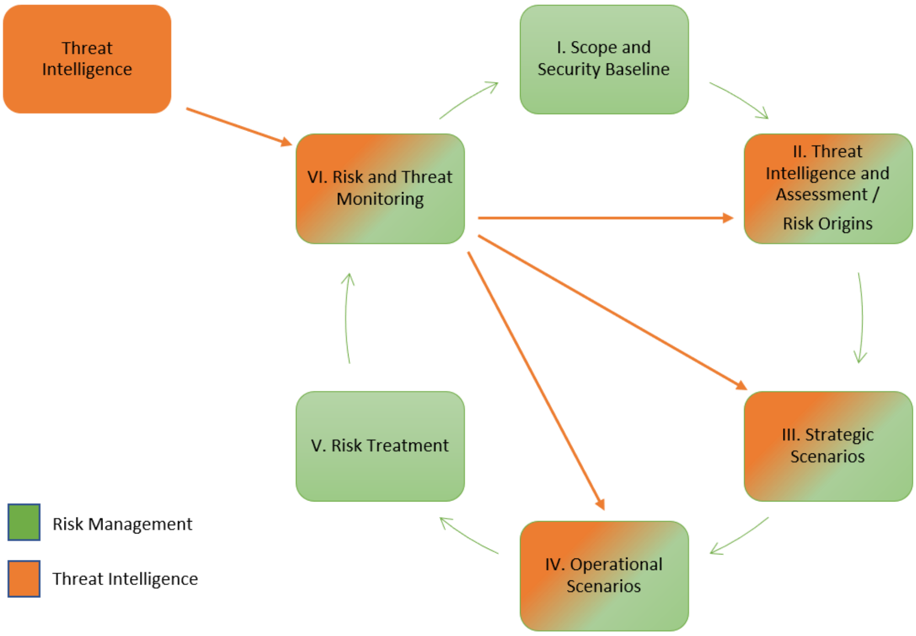
Threat Intelligence
I. Scope and Security Baseline
VI. Risk and Threat Monitoring
II. Threat Intelligence and Assessment / Risk Origins
V. Risk Treatment
III. Strategic Scenarios
IV. Operational Scenarios
🟩 Risk Management
🟧 Threat Intelligence

**Figure 3.** Risk management process integrated with cyber threat intelligence.

## 6. Case study of managing cyber risks

There have been many frameworks for providing guidance and managing the cyber risks of healthcare, such as the NIST framework, the IEC 80001 (for medical devices on a network) by the International Electrotechnical Commission (IEC), and the framework by Health Information Trust Alliance (HITRUST) for regulatory compliance and cyber risk management. A dynamic structural model of an aggregate loss distribution across multiple attacks on a prototypical hospital network was developed. The model is a continuous-time Markov chain. There are many medical imaging devices and patient monitoring equipment on the hospital network. The network was modeled as a mixed random graph, and the equipment or devices were treated as random nodes. A probabilistic graph-theoretical framework was contextualized for hospital network problems, which helps enhance the cybersecurity management strategy in the hospital [23].

The distributed situation awareness (DSA) theory draws on distributed cognition framings of team SA and Neisser's perceptual cycle. The DSA theory provides for the examination of a system as a whole. It substantially benefits nursing practice [24]. A conceptual and empirically tested model and validated instruments were provided to evaluate the impacts of cyber-risk management policies at a hospital on healthcare providers' intentions to resist the electronic medical record (EMR) system. Structural equation modeling (SEM) was utilized to test the proposed model. The SEM structural path includes standardized path coefficients and the significance of the paths based on the *p*-value. SEM is a statistical method of analyzing the complex relationship between variables. It is a mix of factor analysis and simultaneous equation modeling [25]. Wireless Sensor Networks (WSNs) provide vital sign collection and real-time patient monitoring; however, they are vulnerable to cyberattacks. A DL-based attack detection and classification approach was presented with an accuracy of 96.78% [26].

Emerald Healthcare System is a not-for-profit corporation dedicated to developing medical programs, healthcare services, research, etc. The system's three hospital campuses, plus several outpatient facilities, offer a broad spectrum of care. Services provided by over 1550 medical staff members and more than 10,300 employed professionals make Emerald Healthcare System one of the largest healthcare providers in Texas, USA. **Table 9** summarizes cyber risk management, including theories, frameworks, models, and practices in the Emerald Healthcare System.

In theories for managing cyber risks (see **Table 9**), big data analytics and big data technologies are utilized in handling all kinds of big medical and healthcare data. AI/ML/DL methods are employed in analyzing medical and healthcare data, modeling the distribution of a disease, predicting the trend of a new disease, etc. FMEA is utilized in discovering possible failure modes, analyzing their effects, and examining data security (infrastructure, communication security, security management, etc.) in the Emerald Healthcare System. The DSA theory helps examine the healthcare system as a whole (a complex distributed system), which benefits the system, such as bringing benefits to nursing practice. In frameworks for handling cyber risks, both NIST (complied with HIPAA) and ISO (with functions in cybersecurity and healthcare) are employed in the Emerald Healthcare System. In models for managing cyber risks, various models (such as ML/DL models and G&E models) are employed, depending on specific sectors and the specific cyber risks (such as clinical cyber risks and risk-based payment) of the sectors in the healthcare system. Cyber risk management and practices are a continuous and dynamic process and should be unceasingly improved due to new risks. Active threat intelligence supplies it into the process of cyber risk management. Trust and risk are coupled with each other. Trustworthiness establishment and evaluation, risk analysis (qualitative, quantitative, or combined), risk assessment, risk mitigation, etc., are involved in cyber risk management and practices in the Emerald Healthcare System.

**Table 9.** Cyber risk management: theories, frameworks, models, and practices.

| **Aspects** | **Details/examples** |
|---|---|
| Theories for managing cyber risks | Big Data analytics, AI/ML/DL, FMEA, DSA theory |
| Frameworks for handling cyber risks | NIST complied with HIPAA security rules<br>The International Organization for Standardization (ISO) for cybersecurity and healthcare |
| Models for managing cyber risks | ML/DL models for cybersecurity in healthcare, G&E models, clinical risk models, risk-based payment models |
| Cyber risk management and practices | Cyber risk management integrated with cyber threat intelligence<br>Cyber risk management within the trust-risk awareness context |

## 7. Conclusion and future research

This paper provides theories, frameworks, models, and practices of cyber risk management. It focuses on identifying, justifying, and describing certain key issues regarding cyber risks. It also presents a case study of managing cyber risks in healthcare. Big Data analytics, artificial intelligence (AI)/machine learning (ML)/deep learning (DL), FMEA, and the DSA theory have been used in healthcare. Both NIST and ISO have frameworks for risk management and cybersecurity. Risk analysis, risk evaluation, and risk control and reduction are three pillars of risk management.

The risk evaluation can use the qualitative method, the quantitative method, or the combined method.

GTA-based models have advantages over other models in performance and costs when they are used in managing cyber risks. ML/DL models, G&E models, clinical risk models, risk-based payment models, etc., have been used in healthcare. Cyber risk management integrated with cyber threat intelligence and cyber risk management within the trust-risk awareness context has been used in the Emerald Healthcare System. Modeling based on real data examples and the test results of the proposed models, such as DL in the Emerald Healthcare System, is our future research.

**Author contributions:** Conceptualization, CAA; methodology, CAA; formal analysis, CAA and LW; resources, CAA and LW; writing—original draft preparation, CAA; writing—review and editing, LW; visualization, CAA and LW; project administration, CAA. All authors have read and agreed to the published version of the manuscript.

**Conflict of interest:** The authors declare no conflict of interest.

## References

1. MITRE Corporation. MITRE systems engineering guide—risk identification. MITRE Corporation; 2021.
2. National Institute of Standards and Technology (NIST). Security and privacy controls for information systems and organizations (NIST Special Publication 800-53, Revision 5). NIST; 2020.
3. Öbrand L, Holmström J, Newman M. Navigating Rumsfeld’s quadrants: A performative perspective on IT risk management. Technology in Society. 2018; 53: 1-8. doi: 10.1016/j.techsoc.2018.09.009
4. Gonzalez-Granadillo G, Menesidou SA, Papamartzivanos D, et al. Automated Cyber and Privacy Risk Management Toolkit. Sensors. 2021; 21(16): 5493. doi: 10.3390/s21165493
5. Kamiya S, Kang JK, Kim J, et al. Risk management, firm reputation, and the impact of successful cyberattacks on target firms. Journal of Financial Economics. 2021; 139(3): 719-749. doi: 10.1016/j.jfineco.2019.05.019
6. Martins AM, Moutinho N. Stock-Term market impact of major cyber-attacks: Evidence for the ten most exposed insurance firms to cyber risk. Finance Research Letters. 2025; 71: 106361. doi: 10.1016/j.frl.2024.106361
7. Wu ZM, Luo J, Fang X, et al. Modeling multivariate cyber risks: deep learning dating extreme value theory. Journal of Applied Statistics. 2023; 50(3): 610-630. doi: 10.1080/02664763.2021.1936468
8. Sun P, Wan Y, Wu Z, et al. A survey on privacy and security issues in IoT-based environments: Technologies, protection measures and future directions. Computers & Security. 2025; 148: 104097. doi: 10.1016/j.cose.2024.104097
9. Kandasamy K, Srinivas S, Achuthan K, et al. IoT cyber risk: a holistic analysis of cyber risk assessment frameworks, risk vectors, and risk ranking process. EURASIP Journal on Information Security. 2020; 2020(1). doi: 10.1186/s13635-020-00111-0
10. Akinwumi DA, Iwasokun GB, Alese BK, et al. A review of game theory approach to cyber security risk management. Nigerian Journal of Technology. 2018; 36(4): 1271. doi: 10.4314/njt.v36i4.38
11. Zarreh A, Wan H, Lee Y, et al. Risk Assessment for Cyber Security of Manufacturing Systems: A Game Theory Approach. Procedia Manufacturing. 2019; 38: 605-612. doi: 10.1016/j.promfg.2020.01.077
12. Sharma BB, Kumar R, Sharma R. Enhancing Smart Grid Efficiency: The Role of IoT Blockchain and Fuzzy Set Theory. In: Optimization, Machine Learning, and Fuzzy Logic: Theory, Algorithms, and Applications. IGI Global Scientific Publishing; 2025. pp. 261-296.
13. Li T, Sun J, Fei L. Dempster-Shafer theory in emergency management: a review. Natural Hazards. 2025; 1-28. doi: 10.1007/s11069-024-07096-w
14. Ksibi S, Jaidi F, Bouhoula A. 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. 2023; 28(1): 107-127. doi: 10.1007/s11036-022-02042-1

15. Shankar DD, Azhakath AS, Khalil N, et al. Data mining for cyber biosecurity risk management – A comprehensive review. Computers & Security. 2024; 137: 103627. doi: 10.1016/j.cose.2023.103627
16. National Institute of Standards and Technology (NIST). The NIST privacy framework: A tool for improving privacy through enterprise risk management. NIST; 2020
17. Facchinetti S, Osmetti SA, Tarantola C. A statistical approach for assessing cyber risk via ordered response models. Risk Analysis. 2024; 44(2): 425-438. doi: 10.1111/risa.14186
18. Kia AN, Murphy F, Sheehan B, et al. A cyber risk prediction model using common vulnerabilities and exposures. Expert Systems with Applications. 2024; 237: 121599. doi: 10.1016/j.eswa.2023.121599
19. Ahn MK, Kim YH, Lee JR. Hierarchical Multi-Stage Cyber Attack Scenario Modeling Based on G&E Model for Cyber Risk Simulation Analysis. Applied Sciences. 2020; 10(4): 1426. doi: 10.3390/app10041426
20. Preston WC. Modern data protection. O'Reilly Media, Inc.; 2021.
21. National Institute of Standards and Technology (NIST). Risk management framework for information systems and organizations: A system life cycle approach for security and privacy (NIST Special Publication 800-37, Revision 2). NIST; 2018.
22. El Amin H, Samhat AE, Chamoun M, et al. An Integrated Approach to Cyber Risk Management with Cyber Threat Intelligence Framework to Secure Critical Infrastructure. Journal of Cybersecurity and Privacy. 2024; 4(2): 357-381. doi: 10.3390/jcp4020018
23. Chiaradonna S, Jevtić P, Lanchier N. Framework for cyber risk loss distribution of hospital infrastructure: Bond percolation on mixed random graphs approach. Risk Analysis. 2023; 43(12): 2450-2485. doi: 10.1111/risa.14127
24. Walshe N, Ryng S, Drennan J, et al. Situation awareness and the mitigation of risk associated with patient deterioration: A meta-narrative review of theories and models and their relevance to nursing practice. International Journal of Nursing Studies. 2021; 124: 104086. doi: 10.1016/j.ijnurstu.2021.104086
25. Samhan B. Can cyber risk management insurance mitigate healthcare providers’ intentions to resist electronic medical records? International Journal of Healthcare Management. 2020; 13(1): 12-21. doi: 10.1080/20479700.2020.1412558
26. Shanmugavelu R, Ravi V. Enhancing Security in Healthcare Frameworks using Optimal Deep Learning-based Attack Detection and Classification for Medical Wireless Sensor Networks. Engineering, Technology & Applied Science Research. 2025; 15(2): 21197-21202. doi: 10.48084/etasr.9741