Journal of Digital Health
https://ojs.luminescience.cn/JDH

LUMINESCIENCE
https://luminescience.cn/

Perspective

A risk strategy, enterprise risk management, and security analytics models

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

[1]Institute for IT Innovation and Smart Health, Mississippi, USA
[2]Institute for Systems Engineering Research, Mississippi State University, Mississippi, USA

*Correspondence: Cheryl Ann Alexander, cannalexander68@gmail.com

Abstract: Risks and risk management are one of the significant aspects in cybersecurity. This paper presents a risk strategy and a strategic vision of cybersecurity and introduces enterprise risk management (ERM), ERM models, and risk management models in healthcare. A case study introducing ERM in healthcare is also presented. The case study includes the ERM framework, common approaches to measuring cyber risks, specific risk metrics and key performance indicators, and cyber threats and cybersecurity enhancement. A strategic vision of cybersecurity should be more oriented to advanced systems and cutting-edge technologies, including intrusion detection systems (IDS), intrusion prevention systems (IPS), big data analytics, blockchain, quantum computing, and artificial intelligence (AI)/machine learning (ML)/deep learning (DL). Risk metrics can use qualitative, quantitative, or hybrid methods. Developing, selecting, and implementing advanced risk metrics using quantitative methods is significant. The Health Insurance Portability and Accountability Act (HIPAA) provides a cybersecurity framework for healthcare.

Keywords: Cybersecurity, Risk metrics, Healthcare, Enterprise risk management (ERM), Artificial intelligence (AI), Digital health

1. Introduction

A risk strategy, enterprise risk management, and security analytics models are significant for the cybersecurity of enterprises, especially in healthcare systems. Risk assessment and risk metrics can use qualitative, quantitative, or hybrid methods [1]. How the development of a risk-averse cybersecurity ecosystem brings value to an organization was discussed. Evidence-based (scientific) methods in cybersecurity risk management should be promoted. Seeking improvements with more quantitative and scientifically sound methods in risk management and decision-making should be encouraged [2].

Many efforts for improvements have been made, and researchers have presented a dynamic systemic approach for cyber risk management of enterprise networks using a principal-agent framework to deal with the relationships between the principal (asset owner) and the agent (cyber risk manager). The principal delegates risk management tasks, such as network monitoring and software patching,

Received: Jul.30,2025; Revised: Oct.20,2025; Accepted: Nov.8,2025, Published: Nov.13,2025

DOI: https://doi.org/10.55976/jdh.42025144088-95

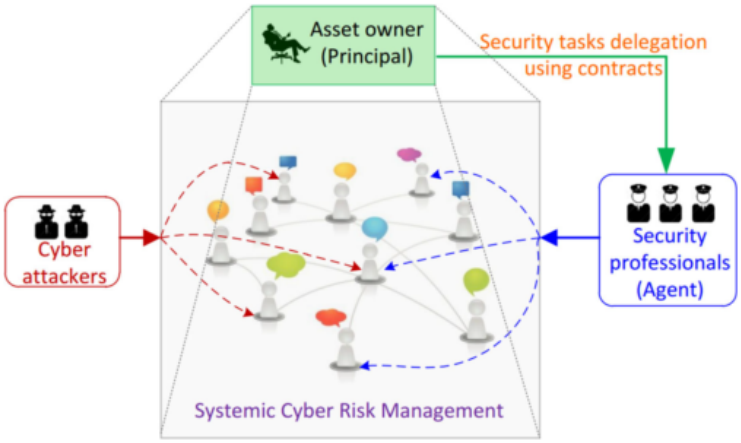

Figure 1. Cyber risk management for an enterprise network [3]

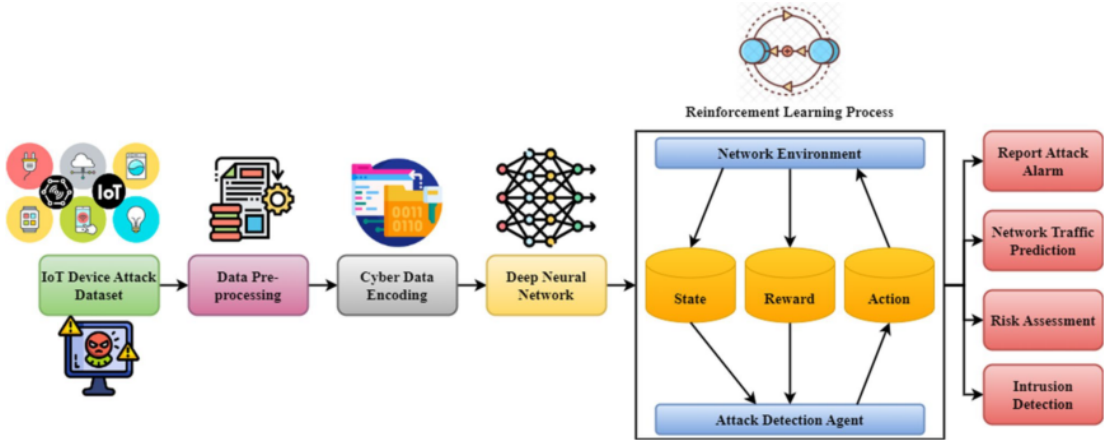

Figure 2. A proposed DRL-NARPP model [4]

to the agent, as illustrated in Figure 1 [3].

Some quantitative and scientifically sound methods in risk management have been developed. For example, a deep reinforcement learning-assisted network awareness, risk perception, and prevention model (DRL-NARPP) has been developed to detect malicious activities in IoT networks. The DRL-NARPP model is shown in Figure 2 [4]. Data pre-processing involves converting raw data into a comprehensible format, including normalizing, standardizing, and scaling data. Cyber data encoding enables feature mapping of a dataset. Researchers have explored the application of reinforcement learning (RL) in network awareness, risk perception, and prevention. [4].

The primary purpose of the research in this paper is to deal with risk strategy and a strategic vision of cybersecurity, ERM, ERM models, and risk management models in healthcare. The remainder of this paper is organized as follows: the second section presents a risk strategy and a strategic vision of cybersecurity; the third section introduces ERM and ERM models; the fourth section presents risk management models in healthcare; the fifth section is a case study of ERM in healthcare, including the ERM framework, common approaches to measuring cyber risks, specific risk metrics and key performance indicators, and cyber threats and cybersecurity enhancement in the Emerald Healthcare System in Texas, USA; the sixth section is the conclusion.

2. A risk strategy and a strategic vision of cybersecurity

A security intelligence model can be implemented as part of a cybersecurity strategy. The Open Systems Interconnect Model is shown in Figure 3 [5]. The security intelligence model is the same as the Open Systems Interconnect Model. It is designed to be operated completely each time it is employed to achieve optimal effectiveness. A user of this model starts in the upper left, goes down to the bottom left, proceeds to the bottom right through the physical medium for interconnection,

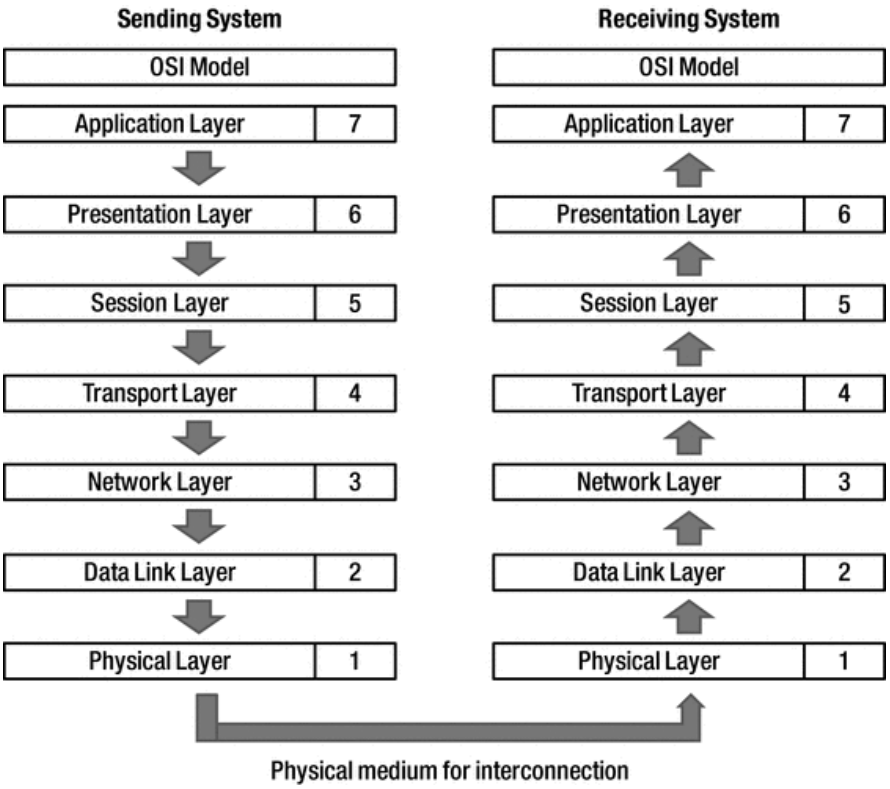

Figure 3. The open systems interconnect model (used as a security intelligence model) [5]

Table 1. Comparison between ERM and traditional risk management

ERM	Traditional risk management
Integrated	Fragmental
Strategic	Tactical
Proactive	Reactive
Non-punitive	Disciplinary
Interdependent	Independent
Consultative	Transactional
Value creation	Asset preservation
Value-based	Cost-based
Organization-wide	Department/silos
Carried out with a process logic	Functional
Continuous & frequent	Discontinuous & not frequent
Top-down, bottom-up, & board/C-suite	Practitioner/Staff

and then goes up, ending in the upper right of the security intelligence model [5]. A strategic vision of cybersecurity lies in adopting or utilizing advanced systems and technologies, including IDS/IPS, big data analytics, blockchain, AI/ML/DL, and quantum computing.

3. ERM and ERM models

ERM is an integrated and holistic approach to risk management that enables an organization to be more strategic. Table 1 [6] shows a comparison between ERM and traditional risk management. The bow tie is a risk analysis and management tool utilized in ERM. It is a visual risk assessment tool that features the concepts of fault and event trees employed in quantitative risk assessment and has been used in various industries. However, it has not been applied widely in healthcare [6].

Many professionals consider risk management (RM) a holistic method. The holistic approach to RM, developed from a comprehensive perspective and employed by companies, is called enterprise risk management (ERM). ERM is presented as a cutting-edge method for controlling the risks of organizations. Data mining has been a very

practical technology in ERM. ERM is categorized into four levels, as shown in Table 2 [7].

Various maturity models for cybersecurity risk management in an organization are described, as illustrated in Figure 4 [2]. The details are listed as follows [2]:

- The operational security metrics maturity model: a matrix of standard questions and data sources.
- Sparse data analytics (SDA): Quantitative methods are used to model risks based on limited data at the earliest metrics stage for new security investments.
- Functional security metrics: Aim to optimize the effectiveness of vital operational security areas.
- Security data marts: Measure across security domains using large datasets.
- Prescriptive security analytics: Provide optimized security recommendations for decision-making.

Table 2. Levels of ERM

Levels	Descriptions
Level 1 (Basic)	Compliance with laws & declarations Guaranteeing compliance with internal controls & avoiding losses Performing subjective or qualitative risk analysis
Level 2 (Standard)	Intensified focus on the risk liability RM activities on a unit basis & in unit-specific area Performing various RM structures & processes Performing tactical RM practices Presenting event-based information & communication Creating fast methods throughout an organization Utilizing semi-qualitative risk models
Level 3 (Modern)	Merging a risk process into a business process Supporting flexibility when abnormal situations occur Attaining intensified focus on future performance Building up a risk-associated information & communication foundation The RM ownership of a management team Creating a worldwide view of the impacts of risk factors on the portfolio throughout the institution & efficiency in RM Connecting qualitative or semi-quantitative models of risk analysis with the elements of creating values for a shareholder
Level 4 (Advanced)	Merging RM into company processes Advocating a risk culture through training Merging scenario & risk analysis into the strategy planning & determination Providing company management with fast information on risk analysis Capital & resource allocation focused on risks, growth, & returns Compatibility of an investor's risk appetite & tolerance with the risk strategy Utilizing the models of risk analysis that permit the prediction of the risk trend and its impacts Establishing the preferences regarding risks, risk distribution, & returns based on the markets of investors, debts, & insurance.

Proactively recognizing and dealing with risks is urgent. A model that significantly contributes to risk resilience throughout the enterprise security risk management cycle is illustrated in Figure 5 [8, 9].

4. Risk management models in healthcare

An AI model was proposed to manage risks in healthcare institutions. A trendy data source, social media, and user interactions are utilized in the model to identify or assess potential risks. Natural language processing (NLP) was applied to analyze users' tweets. Big data analytics (BDA) was employed for the dimensional reduction of data and effective data management. A framework linking risk management, healthcare, and BDA of social media was presented, including risk monitoring, identification, assessment, and control in the framework [10]. The effectiveness of ERM models in healthcare can be measured using qualitative, quantitative, or hybrid methods.

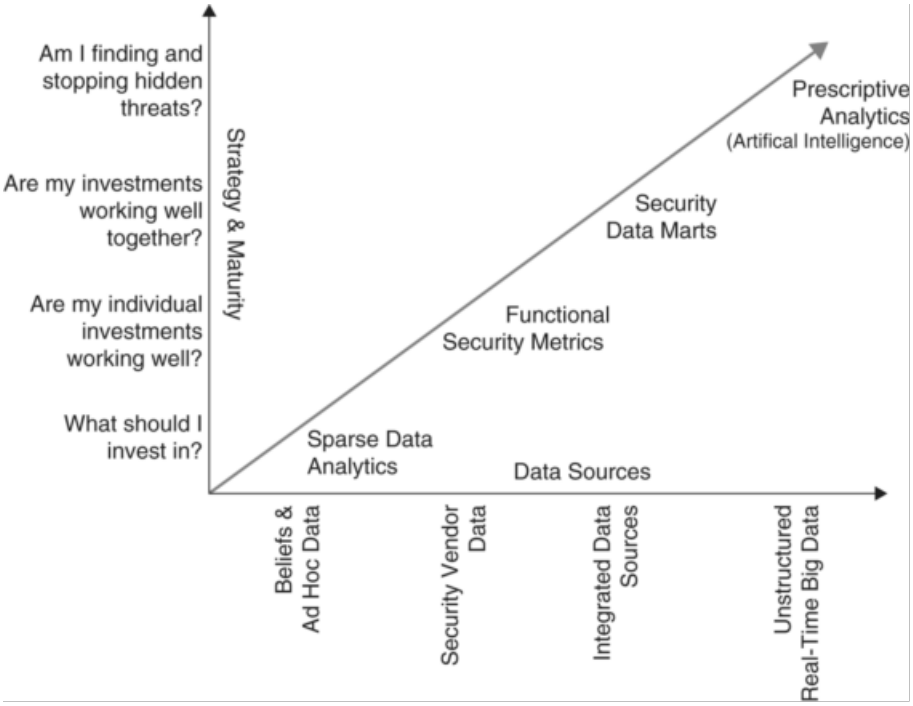

Figure 4. Security analytics maturity models [2]

Figure 5. An enterprise security risk management cycle [8, 9]

Blockchain for healthcare risk management was studied in a conceptual model of information management for managing healthcare risks, and how blockchain can solve concurrent problems in the management of healthcare risks was also explored. Figure 6 [11] presents a proposed risk management process.

The clinical risk management (CRM) model was proposed based on root cause analysis (RCA), failure mode and effects analysis (FMEA), and the systems engineering initiative for patient safety (SEIPS) model. The cumulative burden of healthcare-related adverse events (HAEs) reflects both the severity and the rate of each HAE and has been proven to be a useful output parameter of the CRM model. The elements of the CRM model are shown in Table 3 [12].

5. A case study of ERM in healthcare

Figure 6. A risk management process [11]

Table 3. Elements of a CRM model

Groups of elements	Entities
Management resources	Healthcare tasks Healthcare workers & patients Organizational conditions Internal environment Technologies & tools
Information sources	Administrative data Patient feedback Autopsies HAE triggers Healthcare worker reports Quality & safety walk-rounds Electronic & paper-based medical documentation
Risks (HAE types)	Adverse drug reaction Hospital-acquired infection Blood transfusion complication Perioperative complication Medical device-related complication Etc.
Examples of intervention	Patient Education Healthcare workers training Policies & procedures Equipment upgrade Increased staffing Business process standardization Implementation of clinical decision support systems
Resulting parameters (output)	Rate of preventable HAE Cumulative HAE burden

Emerald Healthcare System is a not-for-profit corporation dedicated to developing medical programs, healthcare services, and research. The system's three hospital campuses, plus several outpatient facilities, provide a broad spectrum of care. Services provided by over 1,550 medical staff members and more than 10,300 employed professionals make Emerald Healthcare System one of the largest healthcare providers in Texas, USA.

The ERM framework in the Emerald healthcare system

ERM offers many benefits. In the Emerald Healthcare System, ERM provides 1) a complete framework intended for making risk management decisions; 2) superior efficiency; and 3) improved risk management, providing an all-inclusive and interconnected visibility into risks and efficient allocation of resources for managing risks. To help entities assess, identify, and prepare for probable cyber risks, the ERM model provides a substantial framework in the Emerald Healthcare System that lays out procedures, processes, and instruments for governing risks at the enterprise level. It functions in the following manner:

- Tailored risk assessment: ensures customized risk management practices for different units.
- Holistic risk management: provides inclusive visibility, which is crucial for successfully and steadily managing risk across the healthcare system.

HIPAA implements controls to secure and protect the privacy of electronic health information and provides a cybersecurity framework that requires healthcare organizations to establish controls for safeguarding and protecting the privacy of electronic health information. HIPAA is implemented in the Emerald Healthcare System.

Common approaches to measuring cyber risks in the Emerald healthcare system

- Perform comprehensive assessments on risk and vulnerability. Risk assessment includes risk analysis and risk prioritization. Risk analysis can involve qualitative and quantitative risk models to analyze the impact and likelihood of cyber threats.
- Both quantitative and qualitative risk models are used. Qualitative analysis maps specific risks depending on their probability of occurrence (very low to very high) as opposed to their impacts (very low to very high). A risk with "high impact, high probability" indicates a severe risk that needs immediate remediation. Quantitative risk assessment measures a cyber risk (from a statistical perspective) to quantify a precise cost or likelihood of the incidence of the risk.

Specific risk metrics and key performance indicators in the Emerald healthcare system

To guarantee the security of data and the safety of the healthcare system, the Emerald Healthcare System uses metrics and key performance indicators (KPIs). Metrics can be used to track quantitative data to ensure the protection of data and other technological assets. Popular cybersecurity metrics and KPIs in the Emerald Healthcare System include the number of security incidents, phishing attacks, intrusion attempts, mean-time metrics and KPIs, such as mean-time to detect, mean-time to respond, and mean-time to resolve.

Cyber threats and cybersecurity enhancement in the Emerald healthcare system

The top cybersecurity threats in 2024 are ransomware, social engineering, third-party exposure, and artificial intelligence cyber threats. Instances of healthcare cyber threats include ransomware, social engineering attacks, third-party data breaches, phishing, and hacking of IoMT (Internet of Medical Things) devices. For example, insulin pumps, pacemakers, or other IoMT devices can be hacked to dangerously alter their functions. Such IoMT devices can be fatally hacked or hijacked. Phishing is one of the most predominant cybersecurity threats in healthcare.

The protection of patient data is one of the primary and crucial roles of cybersecurity in healthcare. The Emerald Healthcare System uses strong passwords, changes them regularly, employs firewalls, installs and maintains anti-virus software, controls access to protected health information and protects mobile devices to improve cybersecurity in healthcare.

6. Conclusion

Because cybercriminals also use advanced technologies such as AI, a strategic vision for cybersecurity should be more oriented to advanced systems and cutting-edge technologies, including IDS/IPS, big data analytics, blockchain, AI/ML/DL, and quantum computing. The benefits of ERM and maturity models should be explored for specific cyber risk environments. Risk metrics can be qualitative, quantitative, or in hybrid methods. Developing, selecting, and implementing advanced risk metrics using quantitative methods is significant and should be encouraged in many situations. Protecting patient data is one of the primary and crucial roles of cybersecurity in healthcare. HIPAA implements controls to secure and protect the privacy of electronic health information, providing a cybersecurity framework for healthcare. There is much work to do on how to achieve the strategic objective and what additional methodologies or tools should be developed. Although part of the strategic objective has been achieved or is being achieved, some methods or tools are still under development to complete the fulfillment of the strategic objective, which is a limitation of this study.

Acknowledgement

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

Conflict of interest

The authors declare that there is no conflict of interest.

Funding

No external funding was received for this research.

Authors' contributions

Conceptualization: CAA, LW; writing the original draft: CAA; manuscript editing, reviewing, and revisions: CAA, LW.

Availability of data and materials

Not applicable.

References

[1] He L. Assessing the smart city: A review of metrics for performance assessment, risk assessment and construction ability assessment. *Cogent Economics & Finance*. 2023; 11(2):2273651. doi: 10.1080/23322039.2023.2273651.

[2] Hubbard DW, Seiersen R. *How to measure anything in cybersecurity risk*. John Wiley & Sons; 2023.

[3] Chen J, Zhu Q, Başar T. Dynamic contract design for systemic cyber risk management of interdependent enterprise networks. *Dynamic Games and Applications*. 2021;11(2):294-325. doi: 10.1007/s13235-020-00363-y.

[4] Xie J. Application study on the reinforcement learning strategies in the network awareness risk perception and prevention. *International Journal of Computational Intelligence Systems*. 2024;17(1):112. doi: 10.1007/s44196-024-00492-x.

[5] Wittkop J. *Building a comprehensive IT security program: practical guidelines and best practices*. Apress Berkeley, CA; 2016.

[6] Elamir H. Enterprise risk management and bow ties: going beyond patient safety. *Business Process Management Journal*. 2020;26(3):770-85. doi: 10.1108/BPMJ-03-2019-0102.

[7] Akbaş MÇ. Measuring the impact of enterprise risk management on performance, value, and risk indicators of Borsa Istanbul XBANK companies with data mining prediction models. *Humanities and Social Sciences Communications*. 2024;11(1):1-9. doi:10.1057/s41599-024-03871-z.

[8] Allen B, Loyear R, *Enterprise security risk management: concepts and applications*. Rothstein Associates, Incorporated, Brookfield, Connecticut, USA, 2017.

[9] Marquez-Tejon J, Jimenez-Partearroyo M, Benito-Osorio D. Security as a key contributor to organisational resilience: a bibliometric analysis of enterprise security risk management. *Security Journal*. 2021;35(2):600. doi:10.1057/s41284-021-00292-4.

[10] Darwiesh A, El-Baz AH, Abualkishik AZ, Elhoseny M. Artificial intelligence model for risk management in healthcare institutions: towards sustainable development. *Sustainability*. 2022;15(1):420. doi: 10.3390/su15010420.

[11] Chung IB, Caldas C. Applicability of blockchain-based implementation for risk management in healthcare projects. *Blockchain in Healthcare Today*. 2022;5:10-30953. doi: 10.30953/bhty.v5.191.

[12] Kleymenova E, Matrosova E, Yashina L, Nazarenko G, Gerasimova N. Systemic approach to the clinical risks management in a healthcare organization. *Procedia Computer Science*. 2022;213:385-90. doi: 10.1016/j.procs.2022.11.082.