International Journal of Business Analytics and Intelligence
12 (1) 2024, 34-39
http://publishingindia.com/ijbai/

Synthesising Value-Leading Cyber Risk Approaches

Cheryl Ann Alexander*, Lidong Wang**

Abstract

Cyber risks are a key issue for enterprises such as hospitals, insurance companies, and other medical organisations. Theft of patient data can pose a considerable threat to medical organisations. Risk management is a significant component of protecting patient and pharmaceutical information. There are serious shortcomings in the regulatory models if these medical organisations are exposed to cybersecurity risks. While most models describe cyber risks in a "one-size fits all" model, excluding calibrations specific to cyber risks most likely to occur in the organisation, using risk management, cyber risk modelling, a strong framework, and standards found in the NIST can strengthen cyber risk management and prevention of cybersecurity risks. In this paper, we first introduced the principles of risk management and approaches to cybersecurity, then discussed cybersecurity in a large medical centre setting, risk management approaches, cyber risk modelling, applying a framework to the cyber risk program, and standards necessary to prevent risks.

Keywords: Cybersecurity, Information, Cyber Risk, Risk Management, Cyber Risk Modeling, Framework, Standards

Introduction

Cyber risks have become an important issue for organisations such as insurance companies. Regulatory models have shortcomings when insurers are exposed to cyber risks. Most models account for cyber risks in a "one-size-fits-all" fashion, not using calibrations specific to a cyber risk. Using risk factors, correlations, and distributions derived specifically from cyber risk data can improve the performance of a model. It is necessary to consider the practice of cyber risk management both in operational risks and in the underwriting of insurance companies (Eling & Schnell, 2020).

There have been many cybersecurity risk assessment approaches and frameworks that are under deployment in organisations. A critical analysis of the cyber-security risk assessment frameworks suitable for Internet of Things (IoT) systems was presented. Applications of IoT risk assessment frameworks in finance and healthcare were discussed. Four risk frameworks were discussed, including ISO. NIST, OCTAVE, and TARA (Kandasamy et al., 2020). For risk management, we should adopt disaster recovery concepts from information technology across the corporation, identify our weakest links, and apply the constructs rigorously (Sengupta, 2020).

Charleston Regional Medical Centre in the US is a hospital that serves patients from a radius of central to western areas of Mississippi. Patient populations include pediatrics, oncology, adults, geriatrics, and all specialties concerning. At any given time, the patient census may be 900-4,000 patients with approximately 1,000 inpatients. Cyber risks and cyber risk management are a constant concern for information technology specialists. With the patient census so high, cybersecurity risks from internal and external sources can weigh heavily on the hospital framework for cybersecurity prevention. The theft of patient data is a real threat and IT professionals must work diligently to prevent this occurrence.

Principles of Risk Management and Approaches to Cybersecurity

Main principles of risk management include: 1) based on the best available information; 2) transparent and inclusive; 3) tailored to organisational needs; 4) explicitly addresses

* Institute for IT Innovation and Smart Health, Mississippi, USA. Email: cheryl.alexander@techhealthsolutions.org (Corresponding author)
** Institute for Systems Engineering Research, Mississippi State University, Mississippi, USA

uncertainty; 5) dynamic, iterative, and responsive to changes; 6) integral part of processes; 7) facilitate continual improvement; 8) systematic, structured, and timely; 9) part of decision-making; 10) create and protect values; and 11) take into account human and cultural factors (Stankov & Gotseva, 2020). Fig. 1 shows a risk management process that monitors and adapts to internal and external changes (Long, 2023).

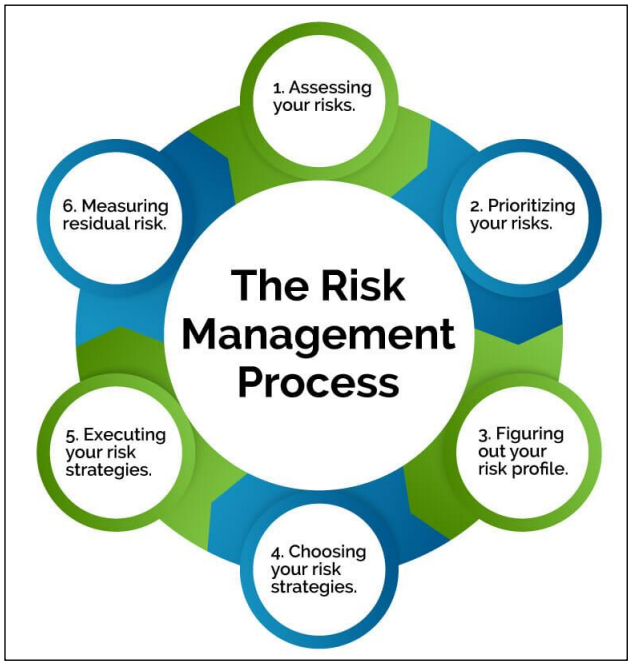

Fig. 1: A Risk Management Process

Implementing effective cybersecurity requires any organisation to identify, prioritise, and manage cyber risks. Risk management requires organisations to 1) frame risks (i.e., establish the context for risk-based decisions), 2) assess risks, and 3) respond to risks once determined, and 4) monitor risks on an ongoing basis using organisational communications and a feedback loop for continuous improvement. Table 1 shows the levels of organisational approaches to risk management and cybersecurity (Marinos, 2019).

Table 1: Organisational Approaches to Risk Management and Cybersecurity

Levels	*Description*
System level	Implement, assess, and monitor security controls Make day-to-day operational risk-based decisions
Mission/ business process level	Define the types of information Define and prioritise mission/business process
Organisation level	Define governance (executive of handling risks) Establish risk management strategy and risk tolerance Evaluate organisation-wide risks

In the Medical Centre, risk management includes management approaches to preventing the theft of patient information, preventing cybersecurity attacks such as Ransomware, and preventing internal hijacking of patient information through the theft of passwords, passcodes, and biometric information such as Pyxis information that guards the medication dispensation and supplies. With the right information, a malicious actor can be a thief of any of these valuable information sources and sell it to the highest bidder. Risk management must be diligent and prevent any such action before it happens.

Cybersecurity is the strategy, policy, and standards regarding the security of operations in cyberspace. It encompasses vulnerability reduction, threat reduction, international engagement, incident response, deterrence, resiliency, and recovery policies and activities. There are six major steps that should be taken to develop and maintain cybersecurity and cyber resiliency strategies. Internal risks can pose as much risk as external cyber risks. The steps are shown in Table 2 (Siegel & Sweeney, 2020). Malicious actors working at the Medical Centre can even steal patient information and sell it to a third party making it nearly impossible for the patient to recoup their losses.

Table 2: Steps for a Cybersecurity and Cyber Resiliency Strategy.

Step Number	*Description*
1	Preplanning: preparation for strategy development
2	Strategy project management
3	Cyber threats, vulnerabilities, and intelligence analysis
4	Cyber risks and controls
5	Current and target state assessments
6	Strategic plan performance measurement and end of the year tasks

Cyber Risk Modeling

A model of cyber risks and quantification has been developed using three key concepts (see Table 3) (Ferbrache & Hanbury, 2020). In the model, the attacker's contact rate is quantified using the number of attackers attempts each year. Cyber risks and attacks are dynamic. In many situations, it is better to use the number of attackers' attempts within a shorter period (e.g., six months or one month). In addition, sometimes it is not easy to quantify the Strength of Foundations because an attacker's success depends on not only weak foundational controls, but also the attacker's knowledge, skills, and methods used. The vulnerability at the organisational level is high. The goal is to reduce threats among internal and external individuals. But deterrence is also high on the list of goals for IT professionals.

Table 3: Cyber Risk Modelling and Quantification using Three Calculation Concepts

Calculation Concepts	*Description*
Threat Quantification	Attackers contact rate (number of attackers attempt each year). Trial & error (the degree to which an attacker is more likely to succeed based on previous attack attempts).
Attack Path Steps Quantification (% likelihood)	Initial compromise (the attacker compromises the environment). Malware deployment (the attacker successfully deploys malware). Lateral movement (the attacker/malware laterally spreads throughout the environment). Evade detection & security response (the attacker evades detection throughout the attack). Action on objectives (the attacker achieves their objectives).
Strength of Foundations	The degree to which an attacker is more likely to succeed due to weak foundational controls.

A conceptual integrative model of organisational resilience was proposed that is shown in Table 4 (Hillmann & Guenther, 2021). In the table, resilience responses substantially depend on resilience resources, capabilities, and behaviours; organisational growth is considerably impacted by resilience responses. It is better to include more elements in resilience resources (e.g., supplies, financial support, and available devices/equipment) and resilience capabilities (e.g., advanced technologies and professionals with skills and experience in resilience) in the table. A resilient, complex, adaptive system based on well-defined operational capabilities and intelligent agents can federate and integrate data, information, or knowledge to help control and manage emerging risks (Butler & Brooks, 2021). In the Medical Centre community, resilience responses substantially depend on the medical centre resources and behaviours of the culture. Organisational growth must also be considered. Cyber risk modelling is very important because it is helpful for making a right decision in time based on the modelling and prediction.

Table 4: A Conceptual Integrative Model of Organisational Resilience

Aspects	*Specific Information*
Resilience resources	Cognitive Emotional Structural Relational
Resilience capabilities	Sensemaking Anticipation
Resilient behaviours	Questioning reality Acceptance Addressing denial Embracing paradox Avoidance
Resilience responses	Maintaining access to resources Maintaining functions Resistance Recovery time
Organisational growth	Adaption Renewal Learning

Frameworks and Standards

A cybersecurity framework profile for ransomware risk management has been developed by the National Institute of Standards and Technology (NIST). There are five cybersecurity framework functions, including Identify, Protect, Detect, Respond, and Recover. Ransomware is a kind of malicious attack where attackers encrypt an organisation's data and demand payment to restore access. There are some basic preventative steps that an organisation can take to protect against the ransomware threat. These include: 1) allowing only authorised apps, 2) using antivirus software at all times, 3) use standard user accounts (versus accounts with administrative privileges), 4) restrict personally owned devices on work networks, 5) block access to potentially malicious web resources, 6) pay attention to social engineering, 7) keep computers fully patched, 8) continuously monitor directory services and other primary user stores, 9) assign and manage credential authorisation for all enterprise assets and software, and 10) segment internal networks (Barker et al., 2021).

A conceptual framework (see Table 5) was proposed as one of the building blocks of a resilient complex adaptive system (RCAS) of systems (Butler and Brooks, 2021). At the Medical Centre, cybersecurity is a constant worry for management.

Table 5: A Conceptual Framework of Organisational Resilience

Constituents	*Description*
Goal	The primary purpose of the system and its subsystems.
Boundaries	Bounding features that describe what is captured in the system/subsystems and what is not.
Feedback loop	The cycle of interaction between/among elements, other subsystems, and the external environment helps adaptation/self-correction and action related to outcomes.
Structure	The organisation of elements and related rules.
Elemental functions	Nestedness, operational capabilities, coordination agents, and adaption agents.
Adaptation	(Sub) systems need to adapt/accommodate operational capabilities for any changes.
Homeostasis	A status of balance, equilibrium, or stability after disturbance.

Aligning Information Communication Technology (ICT) disaster recovery with business continuity is complex due to different focusses; therefore, the British Standards Institution introduced British Standard 25777 as a code of practice for ICT Continuity Management. Cybersecurity standards and regulations from the National Institute of Standards and Technology (NIST) and the International Organisation for Standardisation (ISO) have been created (Tistiyani et al., 2023).

A cyber risk plan was made that aimed at an ICT unit using three security standards, including NIST CSF v1.1 as the main framework (for conducting risk management), ISO/IEC 27005: 2018 as a supporting framework (for conducting risk assessments), and NIST SP 800-53 revision 5 as control recommendations to reduce the impact of risks that occur. The advantage of the NIST CSF framework is that it has a structured and planned format and focusses on business development to guide cybersecurity activities as part of risk management. ISO/IEC 27005: 2018 is a standard that provides guidance on implementing information security risk management. NIST SP 800-53 Revision 5 is a standard that provides an informative reference for achieving comprehensive controls (Safitri et al., 2023).

Conclusion

Cyber risks pose a considerable threat to medical enterprises. IT professionals must always be on guard for internal and external threats posed by malicious actors. Theft of patient data can pose such a threat to medical organisations that it could lead to significant monetary damages. The theft of biometric data, passwords, and passcodes all pose a real threat to the security of patient data and pharmaceutical information. IT professionals must use NIST standards to develop a comprehensive cyber risk model to reduce the impact of risks that do occur. Risk management is a significant component of protecting patient and pharmaceutical information.

Acknowledgements

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

Declaration of the Use of AI Tools

The authors declare that they did not use AI tools in writing this paper.

Conflict of Interest

The authors would like to announce that there is no conflict of interest.

Ethics

In this article, ethical principles related to scientific research articles are observed. The corresponding author confirms that both authors have read, revised, and approved the paper.

References

Barker, W., Scarfone, K., Fisher, W., & Souppaya, M. (2021). Cybersecurity framework profile for ransomware risk management (Preliminary Draft) (No. NIST Internal or Interagency Report (NISTIR) 8374 (Draft)). National Institute of Standards and Technology.

Butler, T., & Brooks, R. (2021). Achieving operational resilience in the financial industry: Insights from complex adaptive systems theory and implications for risk management. *Journal of Risk Management in Financial Institutions*, *14*(4), 395-407.

Eling, M., & Schnell, W. (2020). Capital requirements for cyber risk and cyber risk insurance: An analysis of Solvency II, the US risk-based capital standards, and the Swiss Solvency Test. *North American Actuarial Journal*, *24*(3), 370-392.

Ferbrache, D., & Hanbury, J. (2020). *Cyber risk modelling and quantification.* KPMG LLT.

Hillmann, J., & Guenther, E. (2021). Organizational resilience: A valuable construct for management research? *International Journal of Management Reviews*, *23*(1), 7-44.

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

Long, R. (2023). The risk management process: Manage uncertainty, then repeat. Retrieved November 6, 2023, from https://www.mha-it.com/2020/01/29/risk-management/

Marinos, N. (2019). Cybersecurity: Agencies need to fully establish risk management programs and address challenges. *GAO Reports,* 1-112.

Safitri, E. H. N., & Kabetta, H. (2023, August). *Cyber-risk management planning using NIST CSF V1. 1, ISO/IEC 27005: 2018, and NIST SP 800-53 Revision 5 (a study case to ABC organization).* In 2023 IEEE International Conference on Cryptography, Informatics, and Cybersecurity (ICoCICs) (pp. 332-338). IEEE.

Sengupta, S. (2020, July 1). Risk management in an era of extreme uncertainty. *Supply Chain Management Review, 24*(4), 34.

Siegel, C. A., & Sweeney, M. (2020). *Cyber strategy: Risk-driven security and resiliency*. Auerbach Publications.

Stankov, I., & Gotseva, D. (2020, October). *An overview of security and risk management in business intelligence systems.* In 2020 III International Conference on High Technology for Sustainable Development (HiTech) (pp. 1-5). IEEE.

Tistiyani, S., Briliyant, O., & Trianto, N. (2023, August). Tailoring e-Government's ICT readiness for business continuity based on cyber-risk approach. In *2023 IEEE International Conference on Cryptography, Informatics, and Cybersecurity (ICoCICs)* (pp. 1-8). IEEE.