Research Article

Journal of Biomedical Engineering & Innovations

Measuring Internal and External Cyber Risks

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 authors**

Cheryl Ann Alexander,
Institute for IT Innovation and Smart Health,
Mississippi,
USA.

Submitted : 28 Dec 2024; Published : 18 Jan 2025

Citation : Alexande, C. A. & Wang, L. (2025). Measuring Internal And External Cyber Risks. *J Bio Eng Innov 5*(1): 1-6

Abstract

Most large enterprises devote time and resources to information and cyber risk security management (ISM). With security management, enterprises must also perform incident responses (IRs) which help to mitigate the destruction that occurs due to cyber-attacks. This risk assessment fosters a quick restoration of digital services. In the hospital, ISM is much more critical as it is necessary to protect patient data, equipment, and pharmaceuticals. The IR should be vigorous enough to guard assets and patient data from a cyber-attack and promptly restore patient care by staff. Most public institutions should be focused on infrastructure safety and protecting IT systems. However, there is a significant lack of sufficient policies, management practices, risk assessments, cyber risk measurement, and systems of data and information security governance (DISG). Cybersecurity depends on a multi-faceted cybersecurity framework, including support and assurance from various stakeholders. A robust and up-to-date security control and trustworthy measurement methods are useful in locating problems, recognizing enhancement opportunities, and modernizing cybersecurity controls to counter cyber-attacks and risks. Quantitative data loss is not often available, making it more feasible to get a qualitative assessment of ordinal values when cyber-attacks occur. Cyber risk models, therefore, are a normal tool, useful for employing order response models to analyze cyber risks. Cyber risk modeling in the hospital is often from the qualitative point of view allowing that cyber risks always keep positive associations based on a developed risk propagation model. Cyber risks are identified and categorized as internal or external cyber risks from malicious actors. Therefore, the hospitals must allocate resources to a strong and vigorous cyber risk program. In this paper, we discuss these issues and provide examples of internal and external cyber risks.

Keywords : Cyber risk measurement, cybersecurity framework, risk assessment, internal cyber risk, external cyber risk, cyber risk model, cyber risk modeling, hospital

Introduction

Many big organizations invest in information security management (ISM) to safeguard digital assets. With security management, the organizations also practice incident responses (IRs) to mitigate destruction due to attacks and quickly restore digital services. The integration of ISM and IRs presents learning opportunities that bring security benefits including increased awareness of cyber risks, compilation of risk intelligence, removal of flaws in security defenses, assessment of security defensive logic, and enhanced security responses (Ahmad et al., 2019).

In a medical center, ISM becomes even more important as patient data, equipment, and pharmaceuticals must be protected. The IR must be vigorous to protect assets and patient data from an attack and promptly restore patient care by staff. Preventing a lapse in patient care is a critical function of the IR in any large or small medical center. Patient care can be severely hampered and interrupted when a cyber attack occurs. This is why preventing cyber risks before they happen is such an important function.

Many public sectors or institutions are focused on the safety of their infrastructure and IT systems. There is a lack of sufficient policies, management practices, and systems of data and information security governance (DISG). The implementation and application of integrated DISG management and methods help the government in counteracting cybercrimes and ensure its long-term goals towards effectual cybersecurity in public sector data and information (PSDI). DISG is frequently practiced in private sector management (not very often in public sectors). It is a correlated practice and task to protect an organization's critical data that could not be fulfilled in isolation, requiring a systematic and unified method. Reinventing the responsibility and role of a public sector or institution in protecting the PSDI can improve the processes and synergy of data governance (DG) and information security governance (ISG). This helps improve the processes, systems, and mechanisms related to the PSDI collection, storage, classification, and transmission (Masilela & Nel, 2021).

Government regulations and protection of patient data can determine the response that a medical center has for a breach in cybersecurity. Accessibility and functionality of the staff to patient data and equipment is key to a properly functioning medical center. Having information security and a protection program for all data and equipment is an important part of running the medical center. Information security is essential for preventing patient data theft and other cyber attacks against the medical center.

Cybersecurity Frameworks, Cyber Risk Measurement, and Tools and Practices in Promoting Secure Operations

Cybersecurity relies on a multi-faceted framework, including support and commitment from various stakeholders, robust and up-to-date security controls, and trustworthy measurement methods that are useful in finding problems, identifying enhancement opportunities, and updating cybersecurity controls to counter cyber-attacks and risks. A cyber trust index (CTI) framework was presented. It is a method to measure cyber risks, and it only requires ordinal data regarding the severity levels of detected cyber-attacks. The method relies on the construction of a criticality index. The proposed measure is very effective in ranking cyber risk types and prioritizing cyber risks (Facchinetti et al., 2019).

A privacy-preserving method in smart contracts has been proposed for cyber risk measurements employing artificial intelligence (AI) and the blockchain technology that simplify system activities, human interactions, service alerts, fraud claims, and cyber risks (Deebak & Al-Turjman, 2021). A framework was developed for the analysis of permission blockchain rules and regression algorithms. Table 1 shows the NIST Cybersecurity Framework (CSF): functions and key categories (National Institute of Standards and Technology [NIST], 2018).

Table 1: NIST CSF Cybersecurity Framework

Functions	Categories
Identify	• Business environment • Management of assets • Governance • Strategy of risk management • Risk assessment • Supply chain risk management
Protect	• Awareness & training • Protective technology • Data security • Identity management & access control • Information protection processes & procedures • Maintenance
Detect	• Security continuous monitoring • Detection processes • Anomalies & events
Respond	• Response planning • Analysis • Communications • Mitigation • Improvements
Recover	• Recovery planning • Communications • Improvements

While quantitative data loss is not often available, it is feasible to get a qualitative assessment on ordinal values of cyber-attacks' severity based on experts' opinions. Therefore, it is normal to employ order response models to analyze cyber risks. Experts' assessment of the severity levels of cyber-attacks can be treated as a random ordinal variable, for example, medium severity = 1, high severity = 2, and critical severity = 3. Cumulative link models were presented as a suitable instrument for the assessment of cyber risks. These kinds of models only require ordinal data for the response variable, describing the severity of cyber-attacks (not real losses, protecting cyber victims' privacy) (Facchinetti et al., 2023). Figure 1 (Siegel & Sweeney, 2020) shows the cyber risk score per asset, demonstrating how an overall risk score is calculated per asset (people, processes, technology) using another method.

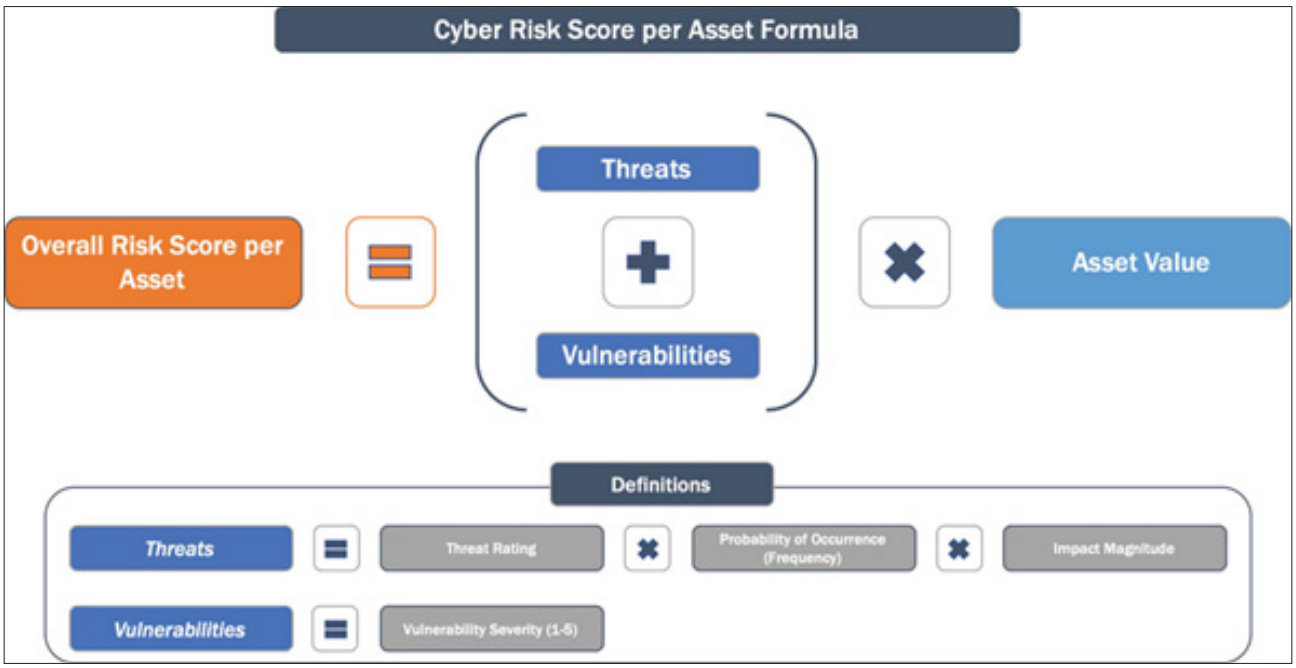

Figure 1: The formula of cyber risk score per asset

Cyber Risk Models and Modeling

An attack and defense game model of a malicious attacker and a defender in the cloud was created. The interactive game process of the attack and the defense was analyzed. The vulnerability of the cloud system was evaluated from the following five aspects: confidentiality, integrity, availability, dependability, and auditability. Security risks of the cloud computing system environment are analyzed (Huang, 2021).

From the qualitative point of view, cyber risks always keep positive associations based on a developed risk propagation model. Cyber risks among the compromise states of nodes over any network are always positively associated based on the L-hop risk propagation model. From the quantitative point of view, an explicit formula used for calculating the fundamental dependence measure of covariance was developed for a network. The impacts of factors—particularly internal and external compromise probabilities, the propagation depth, and the network topology were studied. The dependence on cyber risks is not always increased with the compromise probability or propagation depth (Da et al., 2021).

Qualitative evaluation models for security risks to reflect the security status of a distribution cyber-physical system (DCPS) have been created: for example, a vulnerability evaluation model based on the analytic hierarchy process for urban power grids, cyber security risk evaluation methods for supervisory control and data acquisition (SCADA) systems. Most qualitative evaluation models primarily lack internal links and correlative modeling between various security risk indicators. Quantitative evaluation models have been presented. For example, probabilistic models, a network attack scheme (expressed as a mixed integer linear programming issue) based on the mixture of data integrity and availability, and a dynamic game that assesses the risk of information network vulnerabilities. Most of these models do not disclose the inherent correlations and mutual influences of various risks in the DCPS (Deng et al., 2022).

The loss distribution approach and the time series model were used to measure cyber losses of financial & non-financial divisions. The method of peaks over threshold was also incorporated for an improved risk measurement (Kim & Song, 2023). The model risk and risk sensitivity when dealing with the insurability of cyber risks were studied. The standard statistical approach to the evaluation of insurability and potential mispricing was enhanced in various aspects involving the consideration of the model risk. The model risk can be due to the uncertainties of the model and its parameters. Quantifying the effect of the model risk in the analysis was demonstrated by incorporating various robust estimators for significant model parameters. The relationship between the model risk and the parameter uncertainty in insurance pricing (in the cyber risk setting) was explored (Peters et al., 2023).

How to assess cyber risks and how to design a conceptual model to financially measure the impact of a cyber incident in a bank were studied. A vital outcome of the study is a developed model with steps of quantifying the impact of a cyber incident through eventually decomposing it into several computable metrics. The metrics can be utilized based on the historical cost, or the cost from other organizations. The metrics in the model highlight the areas of extra controls to prevent or reduce such scenarios and inform a needed level of investment into cyber operations and capabilities (Pollmeier et al., 2023).

Measuring Cyber Risks in Hospitals

Cyber threats in healthcare organizations can be categorized as follows: 1) attacks that exploit IT infrastructure vulnerabilities due to misconfiguring network components, e.g., firewalls, denial of service (DoS), structured query language injections, privilege escalation, man-in-the-middle, and cryptographic

attack; 2) ransomware; 3) emerging threats of exploiting human vulnerability in getting access to healthcare infrastructure. It was suggested using international standards ISO/IEC 27002:2013 and ISO 27799:2016 for improving cyber resilience in health care organizations. A risk evaluation method was presented that includes identifying core and mission-critical functions and processes and developing an inventory of vulnerable assets related to the functions and processes. The method permits assigning a risk influence score to a vulnerable asset (Nifakos et al., 2021).

An attack graph is a prevalent modeling method for mitigating cyber-attacks. It can be employed in defending online systems and can be useful for protecting medical and hospital records from cyber-attacks. Some machine learning methods and artificial neural network models have been utilized to model the vulnerability and attacks of industrial control systems. The K-nearest neighbors (KNN) is a successful model utilized in modeling cyber-attacks on the IT system of a health care institution. A common vulnerability scoring system (CVSS) consists of fundamental elements to compute a score: the attack vector, attack complexity, scope, user interaction, required privileges, availability, integrity, and confidentiality (Ünözkan et al., 2022).

Hospitals deal with patients' personal identifiable information (PII) and personal health information (PHI) using electronic health records (EHRs), e-prescription programs, etc. A hospital also utilizes patients' banking and billing information and shares it with insurance companies electronically. A hospital is full of medical equipment or devices connected to the network, and some devices are implanted inside patients. All these are subject to cyber-attacks. Table 2 shows approaches to improving cybersecurity in hospitals (Ahmed et al., 2022).

Table 2: Approaches to improving the cybersecurity of hospitals

Approaches	Description	Threats
Access management policy	Considering unauthorized access to the network	Accidental, intentional, and unintentional data loss; ransomware
Access control of hospital information systems (HISs)	Considering for unauthorized access to HISs	Loss or theft of data
Limiting access to medical devices	Considering unauthorized access to medical equipment	Attacks against connected medical devices
Medical devices security	Considering medical devices and makes sure they are updated	Attacks against connected medical devices
Updated equipment	Considering equipment and its updated status	Loss or theft of equipment
Backup systems	Makes sure data are continuously backed up	Ransomware
Endpoint protection systems	Considering the size of unauthorized data transfers	Loss or theft of data
Email protection systems	Calculates how many spam filters are used for each received email	Ransomware, email phishing
Regular staff training	An employee has cyber threat and security training every year	Accidental, intentional, and unintentional data loss; email phishing
Executing cybersecurity policy	Considering the availability of a policy regarding cybersecurity	All threats

Measuring Cyber Risks in a Medical Center

Charleston Regional Medical Center in the US is a hospital that serves patients from a radius of the central to western parts of Mississippi. Four categories of measurement values are used to measure the cyber risks in the Medical Center, and they are a critical level of severity, a high level of severity, a medium level of severity, and a low level of severity.

Stealing passwords is a critical risk because this will allow others access to patient information and other information about the Medical Center. Passwords are sometimes left stuck on a memo note to the computer when multiple users need access. This is dangerous because a malicious actor can gain access to the computer, thus giving access to valuable information.

Malicious actors try to steal passkeys to all types of locked rooms which can give access to information that could lead to various types of malicious use of patient information, medical equipment, and pharmacy equipment. Sometimes passkeys are in patient care units allowing malicious actors to access locked rooms with records and valuable equipment. These keys must be more protected.

Sometimes staff are careless with their ID badges, or they may leave it connected to a jacket and a contractor or actor may access various departments that have protected information or valuable equipment. These badges must not be left where others can access them. Patient information is very important and must be protected.

While difficult to steal, it is possible to arrange it so that biometric information can be stolen or lifted from pharmacies or supply machines. Once lifted, malicious actors have access to many areas that were previously restricted. With access to the pharmacy, malicious actors can alter drug profiles, and actual medications within the Pyxis dispensation machine, or steal drugs such as morphine or Adderall.

Misuse of patient information is quite common. A staff member may find out that a neighbor or adult relative is hospitalized and feel that it is okay to search the chart for medical information. This is quite illegal and should be cautioned against at all levels.

Data loss occurs by accident. When data loss occurs, the patient suffers. While attacks from the cloud can lead to external data loss, insider data loss occurs when staff misappropriates data, whether from a computer, medical equipment, or a mobile device, data loss must be protected by a strong cybersecurity program.

Emails received by management or staff that may have a cybersecurity risk associated with them. Management should have high security on staff emails so that phishing emails are reduced or eliminated. Staff emails and personal emails can have a great amount of spam mail. It is highly recommended that personal emails be blocked, staff internal emails be monitored for spam mail, and staff be educated on the reduction of opportunities coming from opening spam mail so that cyber risks are introduced to the organization. Educate staff on the risks associated with opening personal emails at work. With the likelihood that personal emails will introduce malicious actors and their schemes to the organization.

Many healthcare facilities have been exposed to ransomware. Once it is introduced and the cyber criminals make the facility aware that their data is now compromised, payment is often the necessary step to recover pertinent and private data. Because patient data are stored in the cloud, malicious actors familiar with operating systems in the cloud can retrieve data and personal data from the cloud, thus compromising the organization's data. Most third parties have their blocks against cyber risks. However, it is pertinent to protect patient data from being compromised further by third parties through excellent cybersecurity practices and programs.

Theft of data or equipment can be a critical cyber risk. Many facilities do not provide protection enough to prevent theft. The organization must provide in-depth cybersecurity protection for data and equipment. Equipment such as ventilators, IV pumps, and other patient equipment can become compromised because they are also connected to the cloud to receive patient information for treatment. Establishing a strong risk management program with cybersecurity is essential.

Much of the medical equipment is connected to the cloud for the treatment of the patient. This equipment is vulnerable to attacks where IV pumps can be set by a malicious actor in the cloud and treatment runs counter to the physician's order. Ventilators that breathe for a patient who is critically ill can also become the victim of a malicious actor who resets the treatment. Other equipment can be adjusted from the cloud and tampered with such as anything with a barcode or connection to the cloud. Table 3 shows cyber risk categories, examples, and cyber risk measuring values in the Medical Center.

Table 3: Cyber risks and their measurement values in the Medical Center

Risks	Examples	Risk Measuring
Internal risks	Stealing passwords (e.g., computer passwords)	Critical
	Stealing passkeys to locked rooms	Medium
	Stealing ID badges	Critical
	Stealing biometric information to pharmacy dispensation rooms	High
	Misuse of patient information by employees and contractors	High
	Insider, accidental, or intentional data loss	Medium
External risks	Phishing emails	Low
	Spam emails	Low
	Ransomware	Critical
	Other cyber risks associated with email and patient information	Medium
	Theft of patient information by third parties through leaks in the cloud	Critical
	Theft of patient information by third parties through leaks in authorized uses of patient information	High
Internal or external risks	The loss or theft of equipment or data	Critical
	Attacks against connected medical devices	Critical

Conclusion

Most larger enterprises invest in an ISM to protect their digital assets from digital threats. Aside from the security management function, most enterprises must also use an IR to moderate damage when an attack does occur so professionals can promptly restore digital access. In a medical center, it is a vital function because, without digital access, many of the medical center's functions cannot run. Security threats must be recognized, and an evaluation of security threats should revolve around vigorous protection of patient data, equipment, and pharmaceuticals. A cyber trust index (CTI) framework was introduced in this paper, and it can measure cyber risks and requires only ordinal data about the severity levels of the observed cyber-attacks. The method relies on the construction of a criticality index. This paper explored the essential concepts and tasks related to prevention of cyber attacks in a medical center.

Acknowledgments

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

Declaration of Conflicting 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

1. Ahmad, A., Desouza, K. C., Maynard, S. B., Naseer, H., & Baskerville, R. L. (2019). How integration of cyber security management and incident response enables organizational learning. *Journal of the Association for Information Science & Technology, 71*(8), 939–953. DOI: https://doi.org/10.1002/asi.24311
2. Masilela, L., & Nel, D. (2021). The role of data and information security governance in protecting public sector data and information assets in national government in South Africa. *Africa's Public Service Delivery and Performance Review, 9*(1), 385. DOI: http://dx.doi.org/10.4102/apsdpr.v9i1.385
3. Facchinetti, S., Giudici, P., & Osmetti, S. A. (2019). Cyber risk measurement with ordinal data. *Statistical Methods & Applications*, 29, 173-185. DOI: https://doi.org/10.1007/s10260-019-00470-0
4. Deebak, B. D., & Al-Turjman, F. (2021). Privacy-preserving in smart contracts using blockchain and artificial intelligence for cyber risk measurements. *Journal of Information Security and Applications*, 58, 102749. DOI: https://doi.org/10.1016/j.jisa.2021.102749
5. National Institute of Standards and Technology (NIST) (2018). Framework for improving critical infrastructure cybersecurity. https://www.nist.gov/cyberframework
6. Facchinetti, S., Osmetti, S. A., & Tarantola, C. (2023). A statistical approach for assessing cyber risk via ordered response models. *Risk Analysis, 44*(2), 425-438. DOI: https://doi.org/10.1111/risa.14186
7. Siegel, C. A. and Sweeney, M. (2020). Cyber Strategy: Risk-Driven Security and Resiliency. *Auerbach Publications*. DOI: https://doi.org/10.1201/9780429323003
8. Huang, M. (2021). Design of basic process of information security risk assessment in cloud computing environment. 2021 IEEE International Conference on Consumer Electronics and Computer Engineering (ICCECE), Consumer Electronics and Computer Engineering (ICCECE), 2021 IEEE International Conference On, 494–499. DOI: http://dx.doi.org/10.1109/ICCECE51280.2021.9342156
9. Da, G., Xu, M., & Zhao, P. (2021). Multivariate dependence among cyber risks based on L-hop propagation. *Insurance: Mathematics and Economics*, 101, 525-546. DOI: https://doi.org/10.1016/j.insmatheco.2021.09.005
10. Deng, S., Zhang, J., Wu, D., He, Y., Xie, X., & Wu, X. (2022). A Quantitative Risk Assessment Model for Distribution Cyber-Physical System Under Cyberattack. *IEEE Transactions on Industrial Informatics, 19*(3), 2899-2908. DOI: http://dx.doi.org/10.1109/TII.2022.3169456
11. Kim, S., & Song, S. (2023). Cyber risk measurement via loss distribution approach and GARCH model. *Communications for Statistical Applications and Methods, 30*(1), 75-94. DOI: http://dx.doi.org/10.29220/CSAM.2023.30.1.075
12. Peters, G. W., Malavasi, M., Sofronov, G., Shevchenko, P. V., Trück, S., & Jang, J. (2023). Cyber loss model risk translates to premium mispricing and risk sensitivity. *The Geneva Papers on Risk and Insurance-Issues and Practice, 48*(2), 372-433. DOI: https://doi.org/10.1057/s41288-023-00285-x
13. Pollmeier, S., Bongiovanni, I., & Slapničar, S. (2023). Designing a financial quantification model for cyber risk: A case study in a bank. *Safety Science,* 159, 106022. DOI: https://doi.org/10.1016/j.ssci.2022.106022
14. Nifakos, S., Chandramouli, K., Nikolaou, C. K., Papachristou, P., Koch, S., Panaousis, E., & Bonacina, S. (2021). Influence of human factors on cyber security within healthcare organisations: A systematic review. *Sensors, 21*(15), 5119. DOI: https://doi.org/10.3390/s21155119
15. Ünözkan, H., Ertem, M., & Bendak, S. (2022). Using attack graphs to defend healthcare systems from cyberattacks: a longitudinal empirical study. *Network Modeling Analysis in Health Informatics and Bioinformatics, 11*(1), 52. DOI: https://doi.org/10.1007/s13721-022-00391-1
16. Ahmed, M. A., Sindi, H. F., & Nour, M. (2022). Cybersecurity in Hospitals: An Evaluation Model. *Journal of Cybersecurity and Privacy, 2*(4), 853-861. DOI: https://doi.org/10.3390/jcp2040043.