Comparative Study of Cyber Security Risk Assessment Frameworks

Details of Author(s) : [1]Swapna Siddamsetti, [2] Dr.Rajasekaran Subramanian
[1]Research Scholar, Department of Computer Science,GITAM Institute of Science,GITAM University,Vishakapatnam,
[1]Assistant Professor,Department of Computer Science and Engineering,Neil Gogte Institute of Technology,Hyderabad, swapnangit2021@gmail.com
[2]Associate Professor,Department of Computer Science and Engineering,Neil Gogte Institute of Technology,Hyderabad, rajasekarans@ngit.ac.in

Abstract-
Cybersecurity risk management is regarded as an essential component of a strategy for risk management because it enables the funding to be allocated to control the most severe risk by establishing priorities. There are several approaches for risk assessment and analysis. Meanwhile, international and national standardization groups reacted by developing multiple risk management for cybersecurity frameworks and standards that firms may use as they mature their network security capabilities. In summary, this study aims to critically assess three cybersecurity risk management frameworks widely used by enterprises to mitigate cyber risks. The article opens with an overview of why businesses should develop a cybersecurity risk control strategy. In addition, the article gives an introduction of some well-known risks associated with cybersecurity strategies, as well as Furthermore, the article identifies the evaluation criteria for making comparisons structures and offers a comprehensive assessment of particular risk management for cybersecurity structures intending to support framework selection decision-making, facilitating pragmatic execution of cybersecurity projects, and assisting organizations in dealing with cybersecurity risks. Finally, the study concludes with some thoughts.

DOI Number: 10.48047/nq.2023.21.6.nq23199 **NeuroQuantology2023;21(6):2015-2024**

INTRODUCTION

Risk management and treating methods are essential for the execution of an efficient security program and are a key component of national and international data protection regulations. A full understanding of cybersecurity risks is essential to guarantee that security precautions are appropriate to give an effective degree of defense against cyber-attacks. Yet, developing trustworthy models for cyber risk exposure remains a challenge. Existing models [1-4] have serious faults, such as limiting the creation of a defense-related market [5]. First, cyber risks evaluation-related impact evaluations occur mostly qualitatively, sometimes impeded by mistakes and misleading statements of the danger. These have substantial disadvantages, such as the imprecise quality of the information acquired and the difficulty of doing a financial analysis [6]. Data analysis techniques are often founded on rating scales that lend a specific score to a technical or organizational context. Although the idea is excellent, however, it will be seen shortly. This same way it is commonly implemented doesn't always offer an appropriate assessment of emerging risks but also their effects. Accurate models for quantifying data breaches will either lack significant shortcomings, including a shortage in generality, or most authors only examine prior information to build statistical methods, having left as unclear to acquire correct estimates regarding future events [7, 8]. Additionally, certain quantitative techniques,

such as the popular HTMA (how to measure anything)
[9] and FAIR [10] methodologies, rely on a subjective evaluation of the chance of an occurrence supplied by an expert team [11, 12]. The estimates were frequently incorrect and might be replaced with objective models. The impact of persistent threats is subsequently assessed using monetary damage, which is appraised subjectively. According to these principles, it is evident that there is a need to enhance the quantitative assessment of an organization's cyber risk through a variable that affects the assaults and vulnerabilities that the business is facing. [13] conducted a recent study on data thefts in the context of technological and network security. Yet, it is clear that the entire picture encompasses numerous sectors (such as commercial and financial enterprises) and other cyber dangers. This suggests extensive research is required to generate credible representations of this large issue. [14] takes a step towards generalizing this work by analyzing sufficiently big and accessible datasets that cover the full range of cyber hazards and related costs. This method is not novel in the studies (see, for example, [8, 15] for research based on data threats): probabilistic models of registered cyber-crime occurrences may be constructed by examining vast amounts of historical data. Yet, as the authors of these publications make apparent, such a strategy has significant limits. Moreover, cybercrime is a continuous and constantly evolving phenomenon: looking merely at previous data is insufficient for solid predictions about future occurrences. Assume a corporation wishes to assess its risk exposure and develop feasible solutions to improve its security regarding cybercrime. Depending on probabilistic models is most likely insufficient in such a circumstance because unique countermeasures and subsequent assault methods must be considered. [12] uses a dynamic model to show potential relations between defenders and attackers to demonstrate this method. Within this framework, every contingency plan was treated like a major update to existing cyber security systems and was granted the accuracy rate; the optimal solution is discovered by analyzing financial statements for the relationship between defenders and attackers. According to the new analysis, the whole cybersecurity scenario, with its varied ensemble of all imaginable actors and occurrences, appears to be a trait that makes creating good probability models difficult. Applications based on real-world case studies, in particular, may depend on the unique qualities of the topics concerned. For example, conducting a hazard analysis that uses descriptive methods will lead to a high level of malware defense measures, yet it cannot prove that safety precautions are effective in combating ransomware attacks. Due to poor prioritization, large resources may be directed onto prone regions that are not as vital and do not justify these assets, and vice-versa. As previously noted, relying on expert opinions minimizes ambiguity in this circumstance [11, 12]. This approach is employed for HTMA [9], which assigns a test statistic and an impact to a set of threats. Fundamentally, the occurrence is the likelihood of such a victorious invasion due to every hazard, while the effect is the resulting economic damage. The HTMA approach, in particular, evaluates its impacts through conversations with specialists who are asked to provide the 90% confidence range on anticipated lost revenues by each danger. These replies are utilized to calculate the probability density connected with the effect; a log-normal distribution is employed for each hazard evaluation. We use the HTMA approach in our study, But it's merely a starting point to be steadily and continuously improved by collecting new and valuable information on the company's actions in the context of cyber threats. Specifically, writers propose utilizing HTMA as an entry combination of probabilistic and objective data. This project aims to create a system for adapting a statistical approach to a case study from the real world. The strategy we provide is largely focused on evaluating the efficacy of implemented treatments using a data-driven methodology. As previous SANS Institution research has shown [16], one of the key objectives of a complete security risk

analysis is analyzing the performance of security measures deployment. Furthermore, an assessment that shows both chance and effect is one common technique for assessing threats, which is apparent in most threat assessment approaches. Previous methodologies reached these values by studying a suitable enough amount of past data. Unfortunately, these numbers rarely represent the status of the item under consideration. Thus, determining the exposure to risk without considering the efficiency of the controls in place is difficult. Our research takes CIS 20 Key Mechanisms of Defence (Center for Cybersecurity, https://www.cisecurity.org/) into account for this purpose, but the same technique may be used for any other relevant set of security concerns.

RELATED WORK

Cybercrime has grown increasingly severe and widespread as a process of globalization, digitization, and smart technology. Despite cybersecurity detection being a developing subject of study and business, the necessity of skills to perform investigative techniques is already underlined at company, national, & worldwide levels. By 2020, poor cybersecurity is predicted will damage a financial system with us$ 945 billion. Maleks Smith and colleagues (2020). Cyber vulnerabilities provide substantial business risks such as disruptions, data leaks, and financial struggles (Sheehan et al., 2019). Due to its increasing importance within the global market, information about hackers is limited. It can be described in several ways.

To begin with, because it is a new and emerging field, previous data sets are restricted (Biener et al., 2015). A lack of knowledge stymies several businesses, particularly investigation, vulnerability assessments, and cybersecurity (Falco et al., 2019). It could be that breached firms will not frequently publicize the occurrences (Eling & Schnell, 2016). A statement by the European Council on April 2021 announcing that a security excellence center would be built that connects defense spending, innovation, and rapid industrialization emphasizes the importance of this issue. This center's mission is to improve the security of all such computer systems and other vital information infrastructures and networks (European Council, 2021). This study offers one risk-based strategy to risk management, concentrating on cybersecurity hazards and examining the role of cybercrime and cyber insurers in risk management and transfer. The study examines recent cybersecurity and cyber event literary works and data freely accessible from sources. It is the thorough initial assessment of current information on cyber risks, particularly cybersecurity. This activity benefits the scientific world by gathering, describing, and categorizing all available open datasets, as well as recognizing and critically analyzing the existing datasets.

Moreover, additional information is being introduced to provide insights and assist financial planning and cybersecurity stakeholders. The discovered available data might help cyber insurance companies develop more sustainable plans. Because of a paucity of historical data, traditional risk assessment methodologies have become ineffective for financial institutions (Sheehan et al., 2021). Due to this unpredictability, hacking insurance providers are more prone to overcharging for threat coverage (Kshetri, 2018). Integrating data sources with data from insurer portfolios appears crucial for improving risk assessment and, as a result, possibility premiums (Bessy-Roland et al., 2021). The fact that certain re/insurers have said that they are attempting to strengthen current cyber pricing structures (for example, by building or getting databases from third-party suppliers) lends credence to this thesis (EIOPA 2018). Figure 1 depicts the pricing techniques and criteria utilized in the insurance companies' model evaluation based on the results of EIOPA (2018) and the Romanosky et al. study (2019). Cyber dangers are all data breaches and their consequences. Apart from the benefit of threat payment, the availability of accessible datasets allows businesses to examine their corporate cyber defenses and cybersecurity practices. These findings may aid in enhancing awareness & commercial practices. Several corporations can estimate the threat posed by cyberattacks

(Leong & Chen, 2020). This report lays the groundwork for policymakers to create a comprehensive inventory of cyber threats. Although many countries require enterprises to report security breaches to the appropriate regulations, such knowledge is rarely available to academics. Moreover, the higher rate of pay for these violations is frequently unknown.

3. A FRAMEWORK RELATED IN CALCULATION OF CYBER SECURITY

A framework provides stakeholders with a vocabulary to comprehend what cybersecurity risk is. It may allow us to recognize what dangers we face and decrease cybersecurity threats, and it can be used as a risk management tool.

National Institute of Standards & Technology. NIST created an approach to safeguarding critical assets, and anybody can use the NIST framework for cyber risk score.

International Organization for Standardization, or ISO. ISO is a non-profit technology company that designs standards in a range of fields, including cybersecurity. The ISO/IEC 2700 series of standards provides a framework for vulnerability management. This approach is advantageous for firms that operate in many countries.

General Data Protection Regulation. The GDPR is a collection of regulations and laws aimed at safeguarding the identifiable data of European Union citizens. The regulations are imposed anytime residents access any website, regardless of the site. Numerous firms throughout the world comply with GDPR rules.

Certification of the Cybersecurity Maturity Model. According to the CMMC, every company interacting with the Defence Department (DoD) must follow a few cybersecurity procedures to secure defense data.

ISO 27001. ISO/IEC 270001 was published by International Organization for Standardization (ISO) in collaboration with the International Electrotechnical Commission (IEC). Its ISO/IEC 270001 information security model comprises a set of guidelines for risk management in computer networks. Companies also employ the ISO 31000 standards, which establish business risk control guidelines.

DoD RMF. This risk-management framework (RMF) of the Department of Defense (DoD) specifies the policies and processes that the DoD must follow to evaluate and control hazards. RMF categorizes risk into six essential steps: pick, perform, assess, sanction, and oversee.

The FAIR Framework. The Factor Analysis of Information Risk (FAIR) approach was designed to assist businesses in assessing, analyzing, and comprehending information hazards. The framework's ultimate purpose is to aid businesses in making educated decisions while developing cybersecurity strategies.

The framework NIST 800-53. The National Institute of Standards & Technology established NIST 800-53, security standards, and methodology. This platform is continually modified and aims to discuss cybersecurity approaches.

2018

Compliance is a more fundamental risk for businesses to comprehend. Either a corporation respects the industry norms and rules or does not. Risk assessments in various linguistic languages are required or strongly recommended by HIPAA, ISO, FedRAMP, & CMMC. Another typical event involves the risk element of a normal being split down by category, which implies that a complete risk evaluation would be relevant and assist in meeting numerous standard portions. Compromising compliance certification raises the risk because each violation can result in monetary penalties, license revocation, or operational restrictions.

3.1 Cyber risk assessment methodologies

Risk Categories. The term risk refers to how easily a hacker may compromise a system. When we hear "cyber-attack," we immediately think of stolen information. Hazards are classified into five types: **Strategic.** Strategic risk denotes the influence of a company's choices on it. A strategic risk assessment, for example, may focus on what risks may hamper, halt, or entirely derail a company's development ambitions in a new area.

Reputational. Every firm values its reputation, but few companies appreciate it more than others. As a result, every type of reputational risk comes under this category.

Operational. When procedures, people, or systems fail, revenue and client retention are jeopardized. Letting consumers wait for delivery or forcing them to negotiate inefficient systems poses a significant operational risk. Consider how the Postal system failed to keep up with the increased traffic caused by Covid-19. The USPS was overwhelmed by exponential demand throughout the holiday season, causing customer dissatisfaction and emphasizing how danger is only sometimes malevolent.

Transactional. There is a transaction risk when a procedure or product is delivered. For example, the legal site Lexology says that acquisitions raise transactional risks since corporations ignore processes while attempting to integrate new corporate systems/processes with those already in place. Because of prescription information, health data, and social security numbers, the healthcare business, which is undergoing several acquisitions, is becoming a prominent target. Furthermore, customers are providing an increasing amount of their health data via digital apps and platforms to follow and communicate with their healthcare providers.

Compliance. Compliance is a more fundamental risk for businesses to comprehend. Either a corporation respects the industry norms and rules or does not. Compromising compliance certification raises the risk because each violation can result in monetary penalties, license revocation, or operational restrictions. Another typical occurrence is for the specific risk of a standard to be split down by category, which implies that doing a full risk assessment will be applicable and assist in meeting numerous standard portions. Risk assessments in various linguistic languages are required or strongly recommended by HIPAA, ISO, FedRAMP, & CMMC.

https://blog.rsisecurity.com/advanced-user-guide- to-cyber-risk-assessment-methodologies/ EVALUATION OF THE RISK:

Risk evaluation. A cybersecurity assessment necessitates the definition of a company's core business objectives and the information technology assets necessary to fulfill those objectives. Identifying computer security threats that may negatively influence those assets, evaluating the likelihood of such assaults occurring, and studying the impact it may also have is labor; in brief, developing an exhaustive picture of the attack surface for specific organizational goals. It helps organizations and system administrators make educated choices regarding what to place and apply protective measures to minimize overall risk to levels acceptable to the organization.

Cyber Risk Assessment Methodologies. Utilizing methods while performing a risk assessment allows assessors to collaborate with the right specialists at each review stage, improving threshold determination and generating accurate scoring systems.

2019

Hazard Analysis. The results of hazard analysis are broad risk rankings. In other words, the hazard ranking of a product or procedure is determined by the likelihood and extent of the attack. Unlike security tool rating, this strategy takes a more systematic approach to risk. During analyzing risks, risk assessment teams employ two primary methodologies:

Preliminary Hazard Analysis (PHA) – PHA does not need a thorough understanding of how the product in issue works. By including SMEs throughout the process, any knowledge gaps that occur are filled. Businesses frequently perform PHAs early in the development process since any ensuing discoveries are less expensive to address. A PHA is not a comprehensive risk assessment; it gives insight into which areas may need greater attention.

Hazard Analysis and Critical Control Points (HACCP) – An HACCP expands on a PHI by carefully examining essential control points. A detailed grasp of the procedures or systems involved is required to conduct a HACCP. Activities, accessibility, or use are limited or monitored at critical control points.

Basic Risk Rating Procedure: basic Risk Ranking. Ranking hazards happen in practically all cyber risk techniques. What differs is the depth of the ratings and how they are determined. Most basic risk

evaluation does not use numerical ratings; rather, the procedure rates risk based on what presents the most severe dangers (in theory) to a company's goals or purposes. In other terms, it is a broad approach to risk assessment.

Decide if either internal or external dangers are the more dangerous.

Examine attack vectors and ensure that services, technology, and policies are regularly updated. Fourth, analyze the commercial implications of the identified risks.

Prioritize the hazards and divide them into urgent worries (those that might significantly impact your business) and latent issues (those that would be bothersome but would not create irreparable damage).

Attack Trees. Attack trees assist in determining the likelihood of possible assaults by evaluating who, how, why, & when theoretical attacks occur. The root of a tree diagram represents the primary objective, with the leaves and branches representing alternative methods an attacker may take to reach that aim. Because each tree has just one root, evaluation teams usually generate many trees when utilizing this approach.

Pipeline Model. Because the pipeline model examines the steps required to conduct a transaction, it is appropriate for analyzing transactional risk. A typical pipeline, for example, might examine activities, communication, stable internet procedures, inquiries procedures, & access control processes.

OCTAVE. Carnegie Mellon University's Software Engineering Institute (SEI) created its Functionally Significant Risks, Property, and Security Risk (OCTAVE). The method prioritizes operational risks above technology difficulties.

3.2 Threat-Based Risk Profiling:

Threat-Based Analysis. Agencies or organizations are now obliged to establish their implementation settings for some of the NIST protection measures, including embedded assignments and selection statements, under existing processes. This method may result in varying security solutions that each organization must examine separately to determine acceptance. Normalizing these criteria allows federal agencies to avoid possible hurdles to maximal cloud adoption by increasing the overall reusing of security authorization packaging from agency to agency and decreasing the degree of work for each authorization.

Security Controls Assessment. The NIST SP 800- 53 controls were decomposed into control elements to allow automation of cooperation in the risk- based process. Controlling items are the most granular system security portions reviewed by NIST SP 800-53A decision statements. Grouping control into controlled items allows it also to be classified into security features with specified, tested flaw checks. This method integrates data from both automated and manual evaluations into the entire risk profiling process.

Risk Profiling. The security controls in NIST SP 800-53, version 4, were linked to the sixteenth (16) NIST Interagency Reports (NISTIR) 8011 capabilities. The goal of NISTIR 8011 would be to offer a method for automated security control evaluations in systems. This may be used for initial evaluations, continuing security authorizations, and continual monitoring.

2020

Risk responsibility. All company members should be concerned about security fears, yet top management is ultimately in charge of risk handling. Comprehensive cyber threat management starts with executive and C-suite awareness. Boards and the C-suite are crucial in assisting their firms in responding to the ever-changing cyber threat scenario. Cyber threats and attacks are getting more umerous and complex, even as the business world grows more associated and digital. Managing cyber threats has become a commercial and strategic requirement in this new context, with more significant stakes than ever. Cybercrime nowadays entails more than just fraud and theft. Cybercrime, as the domain of vast crime syndicates, foreign government-sponsored attackers, and cyber terrorists, spans the risk spectrum, involving service disruption, data corruption or destruction, and even "ransomware" events that actively seek to extract money, access, or company secrets from victims. Because so much is at stake, boards and C-suite executives are increasingly aware that

cyber threats must be handled as a critical business risk, needing a consciousness deeply embedded in the company's current culture. Knowing that the company will be penetrated at some point, leaders should identify the most significant risks and how those risks may jeopardize mission-critical assets. **Types of cyber-attacks and cyber-risk.** Cyber risk is "operational hazards to technical and communication assets that have consequences for data or information managing secrecy, dependability, or integrity" (Cebula & Young, 2010). Cyber-attacks of three types have various direct consequences on their victims: Business disruptions prevent companies from running and result in revenue loss; however, the implications of data theft take longer to materialize due to reputational ramifications and legal expenditures. On the one hand, data breaches can impact both the target and other entities. On the other hand, cyber risk losses are typically minor and independent, but they can also have a lower frequency and a significant effect ('blackout scenario'). As indicated in the concept of cyber events, the cyber risk might be unconnected to hacking attacks: for particular, software applications or natural catastrophes can result in the crystallization of cybersecurity threats through business interruptions without any malicious intent. Cyber-attack may affect businesses: confidentiality, integrity, and availability.

The Countries Which are more Exposed To Cyber Risk. The banking industry is highly exposed to cyber threats in various countries. The International Telecommunication Union (ITU), an U.n organization, publishes a worldwide cybersecurity index. A range of elements impacts their index, such as legal, organizational, and structural contexts, along with training programs and coordination (ITU, 2017). Comprehensive threat data is exceedingly difficult for one to survive. There are both public and private published data, but they are inadequate, have varying coverage, and use different definitions of the internet, analyzing cyber damages problematic. Moreover, statistics on losses are acquired from many sources. and using various methodologies (actual costs, predicted costs, etc.), making comparison difficult.

2021

4. RESULTS

Table1: Results obtained by Classification Methods

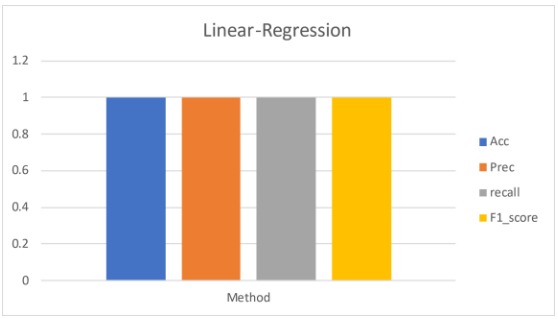


Fig: 1 Performance evaluation of Linear- Regression Method

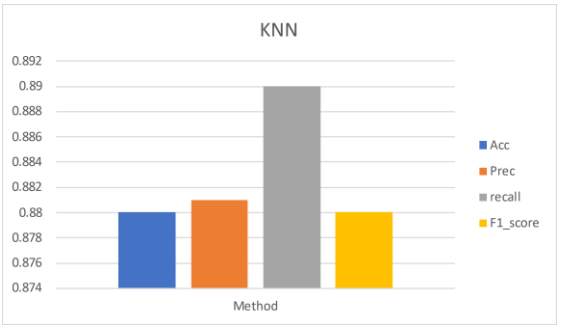
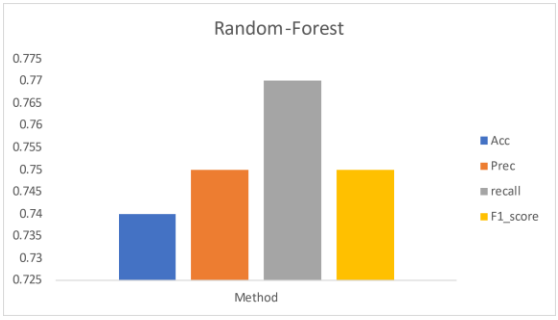


Fig: 2 Performance evaluation of KNN Method



2022

Fig: 3 Performance evaluation of Random Forest Method

Aglorithm	Accuracy	Precission	Recall	F1-score
Linear-Regression	1	1	1	1
Random-forest	0.74	0.75	0.77	0.75
Decision-Tree	-0.17	-0.17	-0.15	-0.15
KNN	0.88	0.88	0.89	0.88
SVM	0.5	0.5	0.54	0.51

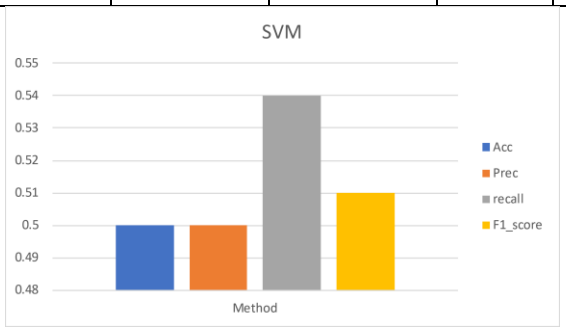


Fig: 4 Performance evaluation of SVM Method

5. CONCLUSION

Several risk assessment methodologies have been created, one of which is more advanced. According to research, the results of risk assessment using existing risk analysis methodologies have beneficial results because they might assist in balancing the losses and costs of enforced procedures. They also help in budgeting and showing the necessity or otherwise of additional investment in information system security. Yet, modernization's influence generates various hazards that cannot be assessed just by quantitative or qualitative techniques. Research is being conducted to develop a more effective risk assessment tool that combines quantitative and qualitative methodologies. Therefore, the described process of current systems is challenging to foresee. There is no comprehensive set that can objectively assess risk to the public and optimize money to fully safeguard an organization's data and assets. Without inquiry and scrutiny, selecting a risk assessment model leads to adopting security measures in the incorrect areas, squandering or abusing resources, and leaving an organization open to unforeseen dangers. An organization Cybersecurity Risks - Management framework, which is simple and explicitly explains a comprehensive safety risks management approach, is required for future work. We will focus on establishing a framework that addresses information security management problems, evaluating the likelihood of incidents, and quantifying their projected damages.

REFERENCE:

1. Roldán-Molina, Gabriela & Almache-Cueva, Mario & Silva-Rabadão, Carlos & Yevseyeva, I. & Basto Fernandes, Vitor. (2017). A Comparison of Cybersecurity Risk Analysis Tools. Procedia Computer Science. 121. 568-575.
2. 10.1016/j.procs.2017.11.075.
3. Dreyling, Richard. (2020). COMPARISON OF CYBERSECURITY RISK ANALYSIS METHODS IN AN E- GOVERNMENT CONTEXT.
4. Giuca, Olivia & Popescu, Traian Mihai & Popescu, Alina Madalina & Prostean, Gabriela & Popescu, Daniela. (2021). A Survey of Cybersecurity Risk Management Frameworks. 10.1007/978-3-030-51992-6_20.
5. Hoffmann, Romuald & Napiórkowski, Jarosław & Protasowicki, Tomasz & Stanik, Jerzy. (2020). Risk based approach in scope of cybersecurity threats and requirements. Procedia Manufacturing. 44. 655-662. 10.1016/j.promfg.2020.02.243.
6. Cremer, Frank & Sheehan, Barry & Fortmann, · & Kia, Arash & Mullins, Martin & Murphy, Finbarr & Materne, Stefan. (2022). Cyber risk and cybersecurity: a systematic review of data availability. Geneva Papers on Risk and Insurance -Issues and Practice. 47. 10.1057/s41288-022-00266-
7. Santini, Paolo & Gottardi, Giuseppe & Baldi, Marco & Chiaraluce, Franco. (2019). A Data- Driven Approach to Cyber Risk Assessment. Security and Communication Networks. 2019. 1-8. 10.1155/2019/6716918.
8. Vorster, Anita & Labuschagne, Les. (2005). A framework for comparing different information security risk analysis methodologies. Pages. 95-103.
9. Cossin, Didier & Lu, Hongze. (2021). Board Oversight of Cyber Risks and Cybersecurity.
10. Ferens, Aleksandra. (2021). Cybersecurity and cyber risk in integrated and management reports of key service operators. Zeszyty Teoretyczne Rachunkowości. 45. 31-50.
11. 10.5604/01.3001.0014.9558.
12. Allodi, Luca & Massacci, Fabio. (2017). Security Events and Vulnerability Data for Cybersecurity Risk Estimation:

2023

Cybersecurity Risk Estimation. Risk Analysis. 37. 1606-1627. 10.1111/risa.12864.
13. Singh, Umesh & Joshi, Chanchala. (2018). Comparative Study of Information Security Risk Assessment Frameworks. INTERNATIONAL JOURNAL OF COMPUTER APPLICATION. 2. 10.26808/rs.ca.i8v2.08.
14. Semlambo, Adam & Lubua, Edison & Mkude, Catherine. (2023). Information Systems Security Policy Framework for enhanced ICT Governance in Public Institutions of Tanzania. 2. 54-68.
15. Zwilling, Moti & Klien, Galit & Lesjak, Dusan & Wiechetek, Łukasz & Çetin, Fatih & Basım, Nejat. (2022). Cyber Security Awareness, Knowledge and Behavior: A Comparative Study. Journal of Computer Information Systems. 62. 82- 97. 10.1080/08874417.2020.1712269.
16. Georgiadou, Anna & Mouzakitis, Spiros & Askounis, Dimitris. (2021). Assessing MITRE ATT&CK Risk Using a Cyber-Security Culture Framework. Sensors. 21. 3267.
17. 10.3390/s21093267.
18. Saleh, Zakaria & Refai, Heba & Mashhour, Ahmad. (2011). Proposed Framework for Security Risk Assessment. J. Information Security. 2. 85-90. 10.4236/jis.2011.22008.
19. Kawanishi, Yasuyuki & Nishihara, Hideaki & Yoshida, Hirotaka & Yamamoto, Hideki & Inoue, Hiroyuki. (2023). A Study on Threat Analysis and Risk Assessment Based on the “Asset Container” Method and CWSS. IEEE Access. 11. 1-1. 10.1109/ACCESS.2023.3246497.
20. Qamar, Sara & Anwar, Zahid & Rahman, Mohammad & Al-Shaer, Ehab & Chu, Bei-Tseng. (2017). Data-driven analytics for cyber-threat intelligence and information sharing. Computers & Security. 67. 10.1016/j.cose.2017.02.005.
21. Bouveret, Antoine. (2018). Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment. IMF Working Papers. 18. 1. 10.5089/9781484360750.001.
22. Mo, Sheung Yin & Beling, Peter & Crowther, Kenneth. (2009). Quantitative Assessment of Cyber Security Risk using Bayesian Network-based model. 10.1109/SIEDS.2009.5166177.
23. Zabawi, A.Y. & Ahmad, R. & Abdul-Latip, Shekh Faisal. (2015). A comparative study for risk analysis tools in information security. 10. 17672- 17678.
24. 6.ACKNOWLEDGMENT
25. Prof. Neil Gogte, Director, Neil Gogte Institute of Technology, Stephen Lobo, Co-founder, CyberGuard360, NC, USA for their support.

2024