Economic Sciences
https://economic-sciences.com
ES(2026)22, 5(S), 661-666 | ISSN:1505-4683

Evaluating the ROI of Cybersecurity Investments through Risk Management Metrics

Dr. Shiva Johri[1], Dr. Raksha Chouhan[2], Dr. Jain Jacob M[3], Dr. Sunil Adhav[4], Prof. (Dr) Sumeet Gupta[5], Harpreet Singh Bedi[6]

[1]Professor & Dean Academics, Department of MBA, Oriental College of Management Bhopal Barkatullah University Bhopal Madhya Pradesh, 50 A Sector Indrapuri, Raisen Road, Bhopal, Madhya Pradesh – 462022. Email:shiva.johri@gmail.com
[2]Associate Professor, Shri Vaishnav Institute of Computer Applications, Shri Vaishnav Vidyapeeth Vishwavidyalaya, Indore, Email:rakshaacademics@gmail.com
[3]Assistant Professor, Faculty of Management, SRM Institute of Science and Technology, Kattankulathur, Chennai, Tamil NaduEmail:jacobjain7@gmail.com
[4]Associate Professor, Department of Business, School of Business, Dr. Vishwanath Karad MIT World Peace University, Pune - 411038. Maharashtra, Email:adhav.sunil2010@gmail.com
[5]Professor and Associate Dean, School of Business, UPES, Dehradun, Uttarakhand Email:sumeetgupta@ddn.upes.ac.in
[6]Associate Professor, School of Electronics and Electrical Engineering, Lovely Professional University Phagwara Punjab India, Email:harpreet.17377@lpu.co.in

Abstract

Associations should make huge interests in online protection arrangements to defend their advanced resources in a period of developing cyberthreats. However, the profit from speculation (return on initial capital investment or ROI) for the vast majority network safety projects is as yet challenging to gauge. This study investigates how risk the board pointers can be used to assess the benefit from adventure for network security utilizations. By getting money related assessment together with risk assessment frameworks, firms can secure a prevalent cognizance of the benefit from their organization insurance hypotheses. This study investigates a digital gamble evaluation process, presents a digital gamble the board structure, and uses a genuine network protection guide to show anincessant improvement of online protection viability and cost of cyber investment examination against the setting of quickly expanding cyberbreaches and the rise of imaginative network protection innovations like AI and man-made brainpower. The outcomes show that utilizing risk the board estimates yield a more exact and nuanced network safety return on initial capital investment evaluation, working with asset designation improvement and very much educated independent direction.

Keywords: *ROI, Cybersecurity, Investment, Risk Management*

<H1> Introduction

It is essential to invest in cyber security given the current condition of network security. Among the many purposes of network security investments are user data protection, financial disruption mitigation, vulnerability correction, and reputation preservation for the company. These expenditures reduce the possibility of fines and closures by enabling organizations to comply with regional laws and ordinances. Organizations can safeguard network and asset integrity and proactively handle changing network issues by making steady and persistent investments in network security (Zamani et al., 2020).

Businesses everywhere struggle to control how growing interconnectedness affects their operations. In actuality, cyber security risk is a crucial component of the overall risk that businesses face, and its significance will only increase. The cost of cybercrime to the world economy has increased by 50% in the last two years, reaching over one percent of the world's GDP, or $1 trillion, according to Allianz world Corporate & Specialty (2021) (AGCS). Meanwhile, the hazards associated with the post-Covid-19 acceleration of digitalization, more serious repercussions from data breaches, and the

Economic Sciences
https://economic-sciences.com
ES(2026)22, 5(S), 661-666 | ISSN:1505-4683

possibility of business disruption due to ransomware attacks, technological malfunctions, or supply chain disruptions loom large. The following important issues are highlighted in this AGCS analysis that analyses cyber risk trends: The volume and complexity of cyber claims are increasing, external attacks result in increasingly costly losses, and internal mishaps happen more regularly. AGCS notes that there are growing repercussions from stricter regulation as well as the possibility of legal action if something goes wrong. "The coronavirus pandemic is an indication that risk management as well as business continuity planning need to further develop in order to help enterprises prepare for, and thrive, extreme events"... "we also have to prepare ourselves for greater numbers of extreme scenarios." Joachim Müller, CEO of AGCS, explains the close connection between pandemic outbreak, interruption of business, and cyber risk.

Estimating the profit from venture (return for capital invested or ROI) of online protection endeavours is as yet troublesome, regardless of its pivotal significance. Network safety programs offer a huge number of advantages and risk alleviations that are habitually neglected by conventional monetary estimations. This dissimilarity makes it more challenging for organizations to conclude how best to dispense their assets to online protection.

<H1> Literature Review

Global underinvestment in cybersecurity, however, continues to be a serious problem. Due to the fact that cyber security does not directly produce income, investment in this area is typically limited (Fedele and Roner, 2022; Lee, 2021). Reducing the sufferers resulting from security occurrences is their goal (He et al., 2022; Smith et al., 2021). The difficulties in measuring return on investment (ROI) and investors' ignorance of the subject exacerbate this (Armenia et al., 2021; Loft et al., 2022). As a result, CISOs and investors from a variety of enterprises now consider security expenditures to be crucial.

It is necessary to consider vulnerability, resources, and the profile of possible attackers in order to obtain a reliable Cy-VaR estimate. A vulnerability is defined by the European Union Agency for Cyber Security as the occurrence of a flaw, design flaw, or implementation issue that may cause an unforeseen event that compromises the information system's security. A single or a sequence of events may be the cause of the unwanted event, which may be certain or uncertain. Users can pose a serious risk to security; in fact, many employees are often the weak spot of an effective cyberattack, either intentional or not (e.g., non-custody of laptop computers storing very sensitive information, unintended release of confidential information). Additionally, the maturity of an organization's security system and its track record of successfully launching successful assaults are the foundations of its vulnerability assessment (Buith and Spataru 2015). Cyber value-at-risk performance is lowered by the absence of industry-wide standardized maturity parameters.

In fact, the result can be an assessment of threat exposure that is subjective rather than objective. In their research, Rabii et al., (2020) provide a thorough overview and synopsis of the emerging topic of security of information maturity ranking through a number of experience reports and case studies.

Finding tangible and intangible assets that are in danger is another fundamental component of Cy-VaR models. Intangible assets, such as human capital, reputation, knowledge, skill, and so on, account for up to 80% of an organization's value and are widely acknowledged as crucial to the functioning of businesses and countries (Dambra and Frumento 2019). Resources must be assessed after identification, which can be challenging when it comes to intangible assets. Asset segmentation into distinct categories, which makes it easier to define the overall security risk, is the last phase. We note that because information assets are unique, it is challenging to estimate the financial and economic consequences of an online attack.

<H1> Methodology

<H2>**A system for managing cyber risks**

A comprehensive approach to cyber risk management must take into account aspects that are both psychological and technological. There are currently many cybersecurity frameworks

Economic Sciences
https://economic-sciences.com
ES(2026)22, 5(S), 661-666 | ISSN:1505-4683

available, such as the Control Objectives for the Protection of Information and Related Technology (COBIT), ISO/IEC 27001, NIST Cybersecurity Framework of Analysis, and ANSI/ISA-624433-3 (99.03.03)-2013. In order to help businesses better manage and reduce cybersecurity risk, the government and industry collaborated to create the NIST Cybersecurity Framework, including consists of optional standards (NIST, 2018). The NIST Cybersecurity Framework, however, barely skims the surface of risk management concerns, including those that are especially relevant to supply chains with external parties.

This article proposed a cyber risk control system that emphasizes the cybercaster along with cyber risk quantification to support existing frameworks such as the Cybersecurity Framework created by NIST and Cyber Kill Chain framework. Four layers make up the suggested framework's classification of the variables influencing cyber risk, and each layer is devoted to particular roles and duties associated with cyber risk administration. Comprising the cybercaster, cyberinfrastructure, cyberrisk valuation, and cyberperformance layers, the suggested framework is depicted in Figure 1. Figure 1 describes each layer in detail

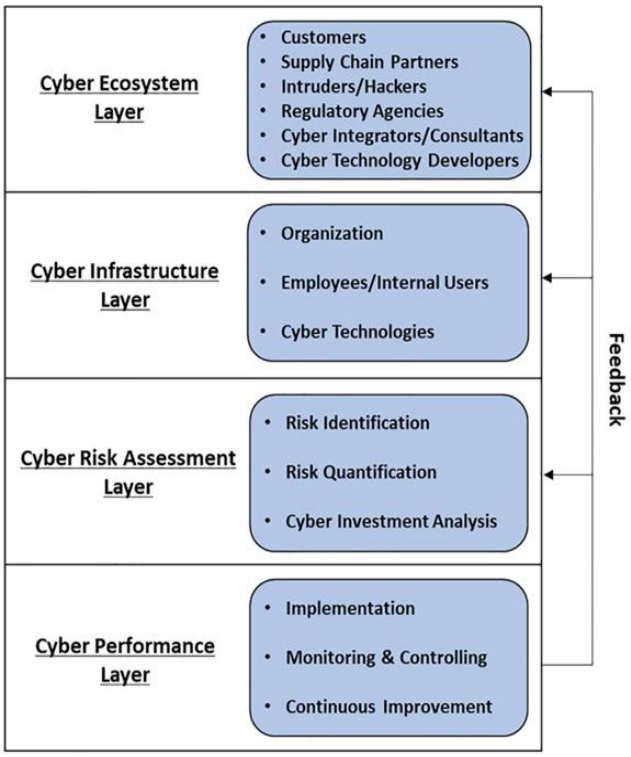

Figure 1: The suggested framework for managing cyber risks; adapted from Lee, (2021)

<H2>**Cyber Risk Assessment**

A key component of the cyber risk management system is the cyber risk assessment layer. A three-step method for comprehending, assessing, and reducing cybersecurity threats is presented by Abraham et al., (2019). Likewise, there are three steps in the layer of cyber risk assessment:

1. Risk valuation, which identifies possible cybersecurity terrorizations, dangers, and outbreaks;

2. Risk measurement, which ranks the different types of attacks and measures their frequency and magnitude; and

3. Cyberinvestment evaluation, which looks at the cost-benefit ratio and helps with cyberinfrastructure investment decisions.

<H2>**Identification of Risks**

Knowing the favoured techniques of hackers and intruders is crucial to spotting cyberthreats. The organization's prior knowledge of the types of

Economic Sciences
https://economic-sciences.com
ES(2026)22, 5(S), 661-666 | ISSN:1505-4683

assets that require protection, as well as the types of threats and vulnerabilities, is reflected in cyber risk taxonomies (Rea-Guaman et al., 2020). The company must develop and maintain the taxonomies that correlate to assets, cybersecurity risks, and cybersecurity in order to facilitate risk detection vulnerabilities throughout time (Rea-Guaman et al., 2020). In order to handle the constantly evolving cybersecurity landscape and continuous or sporadic cyber risk identification, the business must understand the significance of creating and keeping up-to-date taxonomies.

According to Esteves et al., (2017), hackers often go through two stages: exploration and exploitation. In the early phases of an assault, hackers usually engage in an exploration process that relies on extensive testing and blends intentional and intuitive reasoning. Hackers rely on exploitation to accomplish their objectives after gaining access to a system.

<H1> Results and Discussion

<H2>Measuring Risk

The process of creating a cyber risk matrix makes it easier to quantify risks. Assessment team members can help with the quantification process by using a cyber risk matrix. Two dimensions make up the cyber risk matrix. The predicted monetary damage per cyber breach is one dimension, while the frequency of different forms of cyberattacks over time is the other. Not all cyberattacks result in cyber breaches, therefore a cyber breach is a penetration of a cyberattack. It is possible to ascertain the attack-breach risk priority by analysing the risk matrix. Generally speaking, a higher priority will be given to an attack type that is more likely to cause financial damage and that is more common and/or often penetrated.

The lowest projected financial loss and the largest predictable financial cost are caused by the defence likelihood of zero due to cyberattacks (for example, every cyberattack leads to a cyberbreaches). Three different forms of cyberattacks have a defence chance of 1.0 in this cyber risk matrix. The predicted monetary loss of a type I cyberattacks at different defence probability levels, r, is as follows:

$$FL_i = (f_i * l_i)(1 - r) \quad (1)$$

where r is the defensive probability, i is a fixed value, li is a projection of the financial damage of each hacking cyberattack type, fi is an estimation of the type of cyberattack's frequency, and it is also a fixed. It is dependent on investment in cybersecurity.

<H2> Analysis of Cyber Investment

The objective of the cyber rate of investment examination is to reduce the overall cost of the target cyber defensive expenditure as well as the financial damage resulting from computer hacking (i.e., infiltrated cyberattacks). For the cyber investment evaluation to optimize the investment's benefits, it must include the three components of the cyber structures layered organization as well, employees/internal consumers, and cyber technology. The cost analysis of a cyber investment can readily incorporate conventional financial methodssimilar net present value (NPV), return on investment (ROI), and payback methodologies.

In Eqn. (2), the goal function is to curtail the total cybercast, or TC. A cyber investment's cost, D, depends on the likelihood of a defence, r.

$$Min\ TC = D(r) + (1 - r)\sum_{i=1}^{n}(f_i * l_i) \quad (2)$$

As an example, Table 1 uses directed arrows to display the risk profile's progression across two-year periods. Real-world data was modified and used in this risk matrix. The occurrence of assaults and the anticipated monetary cost per interruption are both rising for threats to email systems and network servers. The medium-risk area of the email system transitions to the high-risk area. Desktops and laptops go into the medium-risk category. But although the predicted financial cost per breach rises, the number of attacks falls.

Economic Sciences
https://economic-sciences.com
ES(2026)22, 5(S), 661-666 | ISSN:1505-4683

Table 1: Risk profile evolution during a two-year span

The annual frequency of attacks	Potential Loss of Money (Median Value) for Each Breach in Dollars			Risk Level
	$20000	**$30000**	**$40000**	
> 200	0	Laptop/Desktop	0	Low Risk Area
200	Laptop/Desktop	Email System	0	Medium Risk Area
300	0	0	Email System	
300-400	0	Network Server	0	High Risk Area
400	0	0	Network Server	

<H1> **ROI Calculation**

We took one case study for calculating ROI:Among the serious threats identified in the chief gamble assessment were ransomware, insider threats, and phishing attacks. Ransomware, insider threats, and phishing attacks were found to cost $600,000, $160,000, and $300,000 annually, respectively. The company spent $160,000 on staff planning drives ($27,000), existing email filtering systems ($51,000), and ransomware security programming ($82,000). The following is a quantification of the risk reduction following implementation: With a 70% decrease in phishing attacks, Annual Loss Expectancy (ALE) dropped to $61,000. A 60% decrease in ransomware occurrences brought ALE down to $220,000. A 50% decrease in insider threats brought ALE down to $80,000. The general Lager decrease was $210,000 for phishing, $360,000 for ransomware, $80,000 for insider dangers, and $650,000 for all out-risk decrease.

$$ROI = \frac{Total\ Risk\ Reduction - Investment\ Cost}{Investment\ Cost} \times 100$$

$$ROI = \frac{650000 - 160000}{160000} \times 100 = 306.25\%$$

The Calculated ROI for Cyber Investment is 306.25%.

The network protection endeavours extraordinarily diminished the likely monetary misfortunes from digital assaults, immensely offsetting the costs, as proven by areas of strength for the of 306.25%. The significance of incorporating risk the executives estimate in return for money invested appraisals is featured by this.

<H1> Conclusion

Associations currently must be more mindful of how the network safety scene is changing and respond quickly to it due to the increased dangers that foes and cybercriminals address. This study analysed network safety drifts that line up with changes in mechanical standards. Moreover, this study made the digital gamble the board system, which utilizes four layers to arrange and survey risk the executives' activities. It is fundamental to survey the profit from venture (return on initial capital investment) of network protection endeavours to pursue all around informed choices and apportion assets proficiently. This study shows that adding risk the board estimations offer a dependable method for computing the financial increases from online protection safeguards.

<H1>References

1. Abraham, C., Chatterjee, D., & Sims, R. R. (2019). Muddling through cybersecurity: Insights from the U.S. healthcare industry. Business Horizons, 62(4), 539e548.
2. Allianz Global Corporate & Specialty. (2021). Allianz Risk Barometer 2021: Top Business Risks for 2021. Report. Available online: https://www.agcs.allianz.com/news-and-insights/reports/allianz-risk-barometer.html
3. Buith, Jaques, and Dana Spataru. (2015). The benefits, limits of Cyber- Value-at-Risk. The Wall Street Journal—Business. Available online: deloitte.wsj.com/cio/2015/05/04/the-benefits-limits-of-cyber-value-at-risk/
4. Dambra, Carlo, and Enrico Frumento. (2019). The role of intangible assets in the modern cyber threat landscape: The HERMENEUT Project. European Cybersecurity Journal 5: 56–65.
5. Esteves, J., Ramalho, E., & De Haro, G. (2017). To improve cybersecurity, think like a

hacker. MIT Sloan Management Review, 58(3), 71e77.
6. Fedele, A., & Roner, C. (2022). Dangerous games: A literature review on cybersecurity investments. Journal of https://doi.org/10.1111/joes.12456
7. He, Y., Zamani, E. D., Lloyd, S., & Luo, C. (2022). Agile incident response (AIR): Improving the incident response process in healthcare. International Journal of Information Management, 62(October https://doi.org/10.1016/j.ijinfomgt.2021.102435
8. Lee, I. (2021). Cybersecurity: Risk management framework and investment cost analysis. *Business Horizons*, *64*(5), 659-671.
9. Loft, P., He, Y., Yevseyeva, I., & Wagner, I. (2022). CAESAR8: An agile enterprise architecture approach to managing information security risks. Computers and Security, 122, 102877. https://doi.org/10.1016/j.cose.2022.102877
10. NIST. (2018). Framework documents. Available at https://www. nist.gov/cyberframework/framework
11. Rabii, Anass, Saliha Assoul, Khadija Ouazzani Touhami, and OunsaRoudies. (2020). Information and cyber security maturity models: A systematic literature review. Information and Computer Security 28: 627–644.
12. Smith, R., Janicke, H., He, Y., Ferra, F., & Albakri, A. (2021). The Agile Incident Response for Industrial Control Systems (AIR4ICS) framework. Computers and Security, 109, 102398. https://doi.org/10.1016/j.cose.2021.102398
13. Zamani, E., He, Y., & Phillips, M. (2020). On the Security Risks of the Blockchain. Journal of Computer Information https://doi.org/10.1080/08874417.2018.1538709