Cyber Security Risk Management

Mohammed Mustafa Khan

Abstract

Until organizations establish and implement necessary cyber security risk management programs, they lack assurance that their security controls are operating as expected. Additionally, organizations without cyber security risk management activities are left in the dark. They are not cognizant of information security vulnerabilities and threats impacting mission-critical operations until service disruption occurs. Most organizations mistakenly perform risk management as a one-and-done activity. They conduct risk assessments once and put them aside for a long time as they get engaged in their day-to-day operations; little did they know that their daily operations involved risks. Cyber security risk management is not a destination but an ever-ending journey that ensures the business operations are secure and maintains an acceptable level of risk in case cyber security disasters strike them. The threat landscape is ever-changing, elevating the level of risk for organizations. As organizations shift their operating environments from the Prem environment to cloud and containerized platforms, the attack surfaces are extended; thus, risk exposure is adversely increased with all these transitions. For instance, any time a new device is added to the network, it signals an additional potential risk. Threat exposure has become a dynamic factor, so organizations must normalize evaluating their risk by adopting and implementing a cyber security risk management strategy.

Keywords: Cyber Security, Risk Management, Vulnerability, Threats,

1.0 Introduction

In today's virtual world, cybersecurity risk management has become a field of national and global interest. Companies across different industries rely on information technology to support their key business operations, which exposes them to various cybersecurity threats. Cybercriminals can weaponize these threats and launch attacks that can damage critical systems or wreak havoc in various ways, resulting in data breaches, regulatory fines, loss of revenue, and reputational damage [10]. It is difficult to fully get rid of risks. However, cyber risk management programs can aid in minimizing the consequences and the possibility of threats. Organizations can utilize cyber security risk management to spot their critical threats and choose the appropriate information technology measures to shield information systems against cyberattacks depending on the level of resources, business priorities, and IT infrastructure.

1.1 Problem Statement

Various organizations recognize cyber threats and attacks. However, many organizations are hobbled by managing cyber security risk challenges. The exponential growth of cyber threats combined with IT infrastructure complexities makes implementing and managing powerful cybersecurity measures strenuous. This research paper focuses on how organizations can effectively manage cyber security risk in a dynamic and complex threat landscape.

1.2 Research Objective

This research paper's prime objective is to guide how organizations should develop a comprehensive program for cyber security risk management.

Other objectives include:

- To identify critical elements of cyber security risk management
- To understand modern threat landscapes and how to remediate
- To propose improvements or new approaches to risk management

2.0 Related Work

Cybersecurity risk management has been studied by various researchers, with various frameworks and methodologies developed to address the growing challenges caused by cyber threats. Alshar'e. (2023) performed research on the National Institute of Standards and Technology (NIST) Cybersecurity Framework to evaluate the adoption of the framework. The author found that it is one of the most widely adopted standards. The rationale behind adopting this framework is its ability to discover, assess, and aid in risk mitigation. NIST's framework emphasizes a continuous improvement process, where organizations assess their current security landscape and implement plans to reach their goals. Additionally, the study reported that most small and medium-sized enterprises have not adequately adopted the framework due to limited budget since the framework is resource intensive.

In addition to NIST, the ISO/IEC 27001 standard is another prominent framework that provides step-by-step methods on how to manage sensitive company information and maintain a maximum level of security. ISO 27001 focuses on establishing, implementing, maintaining, and continuously enhancing an Information Security Management System (ISMS). Research performed by Kitsios et al. (2023) indicates that organizations certified under ISO 27001 tend to have better-structured risk management processes, leading to enhanced security architecture.

According to studies carried out by Sinha et al. 2023) on the integration of emerging technologies into cybersecurity risk management. For instance, artificial intelligence (AI) and machine learning (ML) have been applied to automate threat detection and risk assessment processes. Research conducted by Sinha et al. (2024) demonstrates that AI-powered risk management tools can minimize the time required to discover and mitigate cyber threats, thereby improving organizational resilience. However, the adoption of AI in cybersecurity is not without challenges. Issues such as algorithmic bias, lack of transparency, and the need for large datasets to train models can limit the effectiveness of AI-based solutions. Moreover, the integration of AI into existing risk management frameworks requires careful consideration to avoid introducing new vulnerabilities.

3.0 Overview of Cyber Security Risk Management

3.1 Meaning of Cyber Security Risk Management

Cyber security risk management (CSRM) is the process of discovering, assessing, and mitigating possible threats and vulnerabilities to secure the organizational IT infrastructure. It is a fundamental aspect that must be done proactively by organizations to counteract threats before they compromise a system. Organizations can measure the consequences of various threats and prioritize incidence response appropriately by implementing effective CSRM techniques. Effective CSRM enables the implementation of security controls that can act as defense mechanisms in minimizing vulnerabilities and neutralizing possible cyber risks.

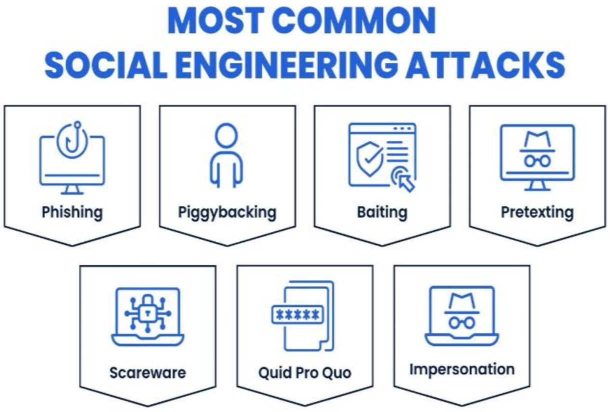
3.2 Common Cyber Security Risks

3.2.1 Malware, Ransomware, and Viruses

Malware, ransomware, and viruses are threats to organizations since cybercriminals capitalize on them to cause data breach incidents and jeorpadize security controls. For instance, in May 2021, a ransomware attack engulfed the Colonial Pipeline Company that stole and locked up the company data [4]. The company could not access their data anymore, and the extortionists demanded a ransom of about 75 bitcoins to pay for the decryption tools required to unlock the data. The control room was forced to shut down some company pipelines to avoid the risk of lateral spread. Indeed, the company experienced detrimental effects that led to financial losses, service disruptions, and critical data loss. This case scenario is a lesson for organizations to implement an effective CSRM program as a countermeasure.

3.2.2 Social Engineering

Social engineering attacks mainly focus on endpoint devices in an organization. Several forms of social engineering attacks, including phishing, smishing, and many more, have been used by cybercriminals [5]. Different tactics can trick the target system or an employee, resulting in devastating impacts on the organization. It is crucial for the CSRM team to deploy strong endpoint security solutions such as SIEM that can detect and respond to threats in real time before causing data breach incidents.



Source: https://www.bitlyft.com/hs-fs/hubfs/Social%20Engineering%20Attacks.jpg?width=1920&height=1080&name=Social%20Engineering%20Attacks.jpg

3.2.3 Insider Threats

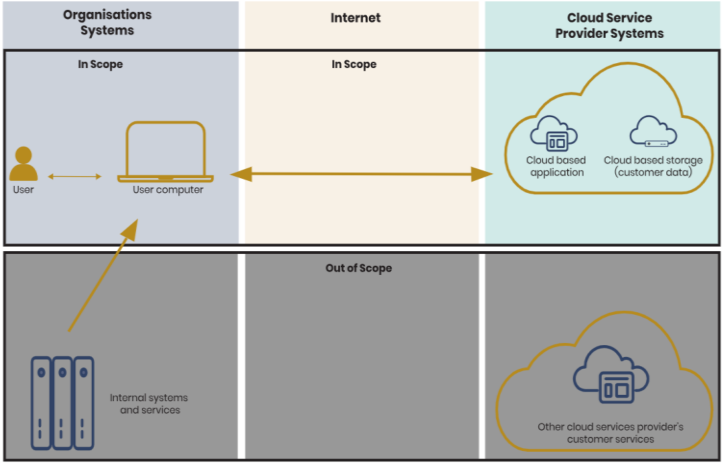
Insider threats are one of the challenging types of cyber risks that are strenuous to detect and discover without implementing advanced threat detection solutions. Insider threats operate as a legitimate entity on behalf of another person since they have gained access to privileged executive accounts and passwords [6]. This normally happens when executive management fails to comply with the best practices for password policy. The insider can steal the intellectual property that is secret to the organization. However, these threats can be detected by advanced threat detection tools since they have the analytic capabilities to identify suspicious user behavior interactions and signal the security teams about the abnormal activity that is happening.

4.0 Basic Cyber Security Risk Management Method

This guidance aims to aid the risk management team in comprehending and managing the cyber security risks impeding their organizations. This section involves a step-by-step process to conduct risk management. It is crucial to master each step to ensure proper implementation of the cybersecurity risk management program. The National Cyber Security Centre provides 11 steps to implement an effective cyber security risk management. This research paper has reviewed all 11 steps and simplified them into five main phases.

4.1 Planning and Preparation

It is a tremendous aspect to outline the scope and the objectives of risk management. Establishing the context for risk management to align with an organization's business objectives and priorities involves defining the program's scope and objectives. A risk management program is a top-down approach whereby all the risk management stakeholders must be included during the implementation process [2]. The risk management team will now gather all the necessary resources and tools needed to conduct risk management, such as an IT asset inventory that helps the team understand the IT assets in an organization. Additionally, this step helps the risk management team to understand the network topology of the organization and comprehend all the system boundaries from one department to another. To understand the scope of risk management, we can utilize a diagram showing how an employee access the cloud-based applications. This further can induce more insights to the risk assessment teams on how entities interact and operate to carry out a successful CSRM.


Organisations Systems
Internet
Cloud Service Provider Systems
In Scope
In Scope
User
User computer
Cloud based application
Cloud based storage (customer data)
Out of Scope
Internal systems and services
Other cloud services provider's customer services

4.2 Assess the Threat

There are various common cyber security risks that have the potential to damage or compromise an organization's information system. This phase helps to identify the adversary behind the threat and the objectives the adversary intends to achieve. Additionally, it may help to understand the tactics attackers can use to gain unauthorized access. Vendors might have historical knowledge of their products pertaining to cyberattacks [2]. However, you do not need to rely on them. It is important to investigate on your own to avoid playing the blame game. Cyber kill chains and other frameworks can tell how threats might attack an organization, as well as tactics and techniques that attackers can leverage to attack the target system within an organization. It is essential to document a list of all known threats to simplify the identification process.

4.3 Vulnerability Assessment

A vulnerability assessment is performed to reveal a loophole that exists in people, processes, and systems. Some different tools and resources can help conduct a successful vulnerability assessment. Tools like vulnerability scanners can be used to perform network reconnaissance. Resources available to the public, such as MITRE's Common Vulnerability Enumeration, can aid in comprehending the known vulnerabilities that affect the system organization's use [2]. Additionally, the resources can provide the geolocation of vulnerabilities and ease in how attackers can exploit a vulnerability. Utilizing various tools and resources is vital to ensure an effective vulnerability assessment. Additionally, physical security measures like access controls, including biometrics, CCTV surveillance, and administrative policies that govern the utilization of IT assets must be evaluated to determine if they meet the ISO standards. Vulnerability assessment helps to identify areas that need rapid attention to seal the flaws.

4.4 Risk Analysis

Risk analysis helps to determine potential vulnerabilities and threats, their possibility and impacts, and the tolerances for such incidents. The outcomes of this process can be shown by utilizing quantitative or qualitative methodologies [2]. Quantitative risk analysis entails arithmetic calculations to locate a value to a possible vulnerability or threat. The predefined formula like ALE (Annualized Loss Expectancy) approximates the reduction in the value of an asset after a disaster occurs, asset value, exposure factor, annual rate of occurrence (ARO), and single loss expectancy (SLE). For example, it is possible to calculate the SLE by finding the product between the asset value and exposure factor [3]. This method is suitable for tangible assets like servers and computers. Qualitative risk analysis methodology assigns a level used to prioritize possible risks so that organizations can use logical steps when addressing the most critical threats. This method applies to intangible assets like intellectual property.

4.5 Responding to Risk

Responding to risk utilizes the aforementioned steps to determine how the organization can counteract the potential risks. Risks that are considered highly unlikely or low-impact risks can be accepted since investing in advanced threat detection tools can be more expensive than the individual risk [2]. The risks with high consequences and likely risks will be addressed using the following risk response metrics:

- Risk avoidance
- Risk mitigation
- Risk Remediation
- Risk transfer

Risk avoidance is the easiest method for minimizing risks. It entails restraining from being involved in risky activities [2]. For example, refusing to download a suspicious email attachment that can maliciously harm the company data. This is a rudimentary solution; some employees may forget to avoid it.

Risk Mitigation may involve the deployment of security controls that detect and disrupt the process of a threat from exploiting a vulnerability or reduce the impact of exploitation [2]. For instance, an intrusion prevention system can be employed to protect an endpoint that stores valuable data.

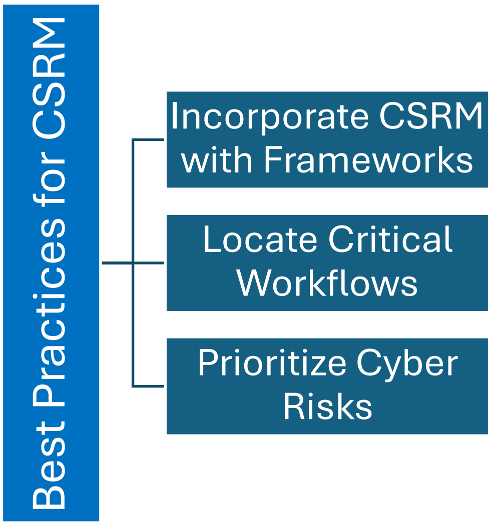
Risk remediation involves hardening the systems so that cybercriminals cannot exploit them [2]. For instance, utilizing the software patches to rectify the existing bugs or decommissioning an obsolete system.

Risk Transfer involves an organization seeking help from another party to protect their IT infrastructure against threats. It takes the form of insurance whereby the organization takes an insurance cover [2]. Doing this can help organization transfer their risk.

4.6 Risk Monitoring and Reviewing

Monitoring helps validate whether the established security controls work as expected and comply with the relevant regulatory requirements. Organizations must monitor and review the IT ecosystems to keep pace with the modern threat attack vectors [2]. Being vigilant on cyber threats improves detection and response time to risk. Reviewing the cyber security risk assessments and controls regularly and improving appropriately on demand is crucial.

5.0 Best Practices for Cyber Security Risk Management



5.1 Incorporate CSRM with frameworks

Several frameworks in the market can act as a roadmap in risk management. It is essential to integrate the CSRM program with these frameworks that can aid in evaluating and categorizing risks [1]. Frameworks are proven methodologies that successfully work to protect the IT infrastructure. Aligning frameworks with cyber security risk management will help organizations establish and implement comprehensive cyber security risk management.

5.2 Locate Critical Workflows

It is imperative to pinpoint the workflows that are of high value to an organization and investigate the associated risk. The processes that generate high business value must be protected at all costs to ensure no service disruption [1]. For instance, workflows that process payment transactions must be thoroughly protected to eliminate fraud activities. These workflows are valuable to the organization and must work as intended with minimal downtime.

5.3 Prioritize Cyber Risks

Ascertain risk level depending on the cost of prevention and information value. High-level risks that are likely to happen must be addressed instantly, whereas lower-level risks wait for later handling, or organizations can accept and tolerate the risk [1]. In the case whereby the asset value is lower than the cost of protection, organizations tend to accept the risk rather than spend a lumpsum amount of money.

6.0 Conclusion

Cybersecurity risk management is a vital component of an organization's overall security strategy. Cybersecurity risks can have devastating effects on an organization. Organizations need to establish and implement a comprehensive cyber security risk management program that aligns with the organizational objectives to enable an organization to attain its vision. Putting into practice each step that has been outlined in the cyber security risk management method and implementing the best practices outline will enhance the protection of their assets and reduce the likelihood of successful cyber-attacks.

7.0 Reference:

1. EC-Council, "Demystifying Risk Management in Cyber Security: Best Practices and Essential Stages Explained," *Accredited Online Cyber Security Degree Programs | EC-Council University*, Aug. 01,

2023. https://www.eccu.edu/blog/cybersecurity/cyber-security-risk-management/

2. National Cyber Security Centre , "A basic risk assessment and management method," *Ncsc.gov.uk*, Jun. 23, 2023. https://www.ncsc.gov.uk/collection/risk-management/a-basic-risk-assessment-and-management-method#section_2
3. Darril Gibson and A. Igonor, *Managing Risk In Information Systems.* SL: Jones & Bartlett Learning, Nov, 2020.
4. A. Hobbs, *The Colonial Pipeline Hack: Exposing Vulnerabilities in US Cybersecurity*. London: SAGE Publications: SAGE Business Cases Originals, Jul. 6, 2021. Available: https://sk.sagepub.com/cases/colonial-pipeline-hack-exposing-vulnerabilities-us-cybersecurity
5. F. Salahdine and N. Kaabouch, "Social Engineering Attacks: A Survey," *Future Internet*, vol. 11, no. 4, p. 89, Apr. 2019, doi: https://doi.org/10.3390/fi11040089.
6. G. Mazzarolo and A. D. Jurcut, "Insider threats in Cyber Security: The enemy within the gates," *arxiv.org*, Nov. 2019, Available: https://arxiv.org/abs/1911.09575
7. M. Alshar'e, "CYBER SECURITY FRAMEWORK SELECTION: COMPARISION OF NIST AND ISO27001," *Applied computing Journal*, vol. 3, no. 1, pp. 245–255, Feb. 2023, doi: https://doi.org/10.52098/acj.202364.
8. A. R. Sinha, K. Singla, and T. M. M. Victor, "Artificial Intelligence and Machine Learning for Cybersecurity Applications and Challenges," *www.igi-global.com*, 2023. https://www.igi-global.com/chapter/artificial-intelligence-and-machine-learning-for-cybersecurity-applications-and-challenges/333785
9. F. Kitsios, E. Chatzidimitriou, and M. Kamariotou, "The ISO/IEC 27001 Information Security Management Standard: How to Extract Value from Data in the IT Sector," *Sustainability*, vol. 15, no. 7, Jan. 2023, doi: https://doi.org/10.3390/su15075828.
10. EC-Council, "How to Effectively Manage Cybersecurity Risk," *Cybersecurity Exchange*, Oct. 08, 2021. https://www.eccouncil.org/cybersecurity-exchange/executive-management/effective-cybersecurity-risk-management-checklist/