Research Article ISSN: 2349-2678

Contents lists available at www.ijpba.in
International Journal of Pharmaceutical and Biological Science Archive
NLM (National Library of Medicine ID: 101738825)
Index Copernicus Value 2019: 71.05
Volume 11 Issue 4; July-August; 2023; Page No. 64-69

Conceptual Development of Cyber Security and Risk Management

Akhilesh[1], Dr. Krishna Dubey[2]

[1]Research Scholar, Sunrise University, Alwar
[2]Professor, Sunrise University, Alwar

Article Info: Received: 15-05-2023 / Revised: 26-05-2023 / Accepted: 29-07-2023
Address for Correspondence: Akhilesh
Conflict of interest statement: No conflict of interest

Abstract

In an era defined by digital connectivity and information exchange, the significance of robust cyber security and effective risk management has become paramount. This abstract presents an overview of the conceptual development of cyber security and risk management, highlighting the intricate interplay between technological advancements, evolving threats, and the imperative to safeguard digital ecosystems. The conceptual development of cyber security and risk management is an ongoing endeavor fueled by technological innovation and threat evolution. As organizations navigate the digital landscape, the integration of these concepts stands as an essential cornerstone for fostering trust, enabling innovation, and safeguarding the digital realms from ever-evolving cyber challenges. The conceptual framework encompasses the comprehensive understanding of cyber security as a multidimensional approach. It encompasses the protection of digital assets, sensitive information, and critical infrastructures from cyber threats. This framework involves the deployment of preventive measures, intrusion detection, incident response, and recovery mechanisms. Additionally, it emphasizes the significance of user education and awareness to fortify the human component of security.

Keywords: Digital, Ecosystem, Technological, Cyber, Security, Threats, Risk, Management

Introduction

A risk landscape is a potent metaphor for the challenges that businesses face as they try to move from their present state to their desired future state. It's also a springboard for contemplating the complex web of relationships between the many entities that make up this environment. Getting a handle on orphan risks is more crucial than ever as businesses adapt to new technology possibilities, changing societal standards, and a fluid dynamic surrounding organizational structures.

Understanding the dangers that may otherwise surprise a company and developing strategies to deal with them is made easier by adopting a "risk innovation mindset.

Risk Management Development

To minimize, monitor, and control the probability or impact of unfavorable events or to maximize the realization of opportunities, risk management entails the identification, evaluation, and prioritization of risks (defined in ISO 31000 as the effect of uncertainty on objectives) and the coordinated and economical application of resources.

Uncertainty in global markets, risks associated with project failures (at any stage of the design, development, production, or maintenance of life-cycles), legal liabilities, credit risk, accidents, natural causes and disasters, malicious attack from an adversary, and events of uncertain or unpredictable root-cause are all examples of risks.

The world is full of both good and negative possibilities, or dangers and chances, respectively. The Project Management Institute, the National Institute of Standards and Technology, actuarial organizations, and the International Organization for Standardization (ISO) have all contributed to the development of standards for risk management. Project management, security, engineering, industrial processes, financial portfolios, actuarial evaluations, and public health and safety all use risk management techniques, but their definitions and objectives are quite different. Despite claims that they reduce uncertainty, several risk management standards have been criticized for failing to reduce risk.

Avoiding, mitigating (lessening the impact or likelihood), offloading (passing the risk to another party), and holding on to (keeping) are all common tactics used to deal with threats (uncertainties with negative consequences). To take advantage of possibilities (beneficial but unknown future circumstances), you might use the inverse of these tactics.

A risk manager's job is to "oversee the organization's comprehensive insurance and risk management program, assessing and identifying risks that could impede the organization's reputation, safety, security, or financial success," and then to "develop plans to minimize and / or mitigate" these adverse (financial) outcomes. Once risk data has been acquired and assessed, analysts discuss their findings with their managers who utilize those insights to pick among alternative solutions. This is the technical aspect of the organization's risk management strategy, and it is supported by Risk Analysts. Financial risk management, internal auditing, and the Chief Risk Officer are related topics. Finance for businesses.

The concept of risk management has been discussed in academic and business journals since the 1920s. In the 1950s, papers and publications with "risk management" in the title began to appear in library catalogs, marking the emergence of the field as a formal discipline. At first, studies focused mostly on economic and insurance topics.

ISO Guide 73:2009, "Risk management. Vocabulary," defines a lexicon that is extensively used in the field of risk management.

Risks that pose the greatest loss (or damage) and have the highest possibility of happening are prioritized in effective risk management. Less likely to occur and do less damage risks are addressed first. As a result, it's very uncommon for practitioners to make mistakes while attempting to strike a balance between mitigating risks that have a high chance of occurrence but a low loss and those that have a low probability of occurrence but a large loss.

A new kind of danger is revealed by intangible risk management: one with a 100% chance of happening but which the company chooses to ignore owing to a lack of identifying capacity. The application of insufficient information to a situation, for instance, would constitute a knowledge risk. When people work together inefficiently, it may put relationships at danger. When inefficient business processes are used, it might increase the risk of process engagement. Knowledge worker productivity, efficiency, profitability, service quality, product quality, brand value, and profits quality are all negatively impacted by these threats. Risk management may provide immediate profit via intangible risk management by identifying and mitigating threats to production.

Risk managers have an interesting problem in the form of opportunity cost. Identifying

whether to invest in risk management and when to allocate funds elsewhere may be challenging. The goal of good risk management is to reduce the likelihood of bad outcomes while keeping costs (or other resources) as low as possible.

Enterprise Risk Management (ERM)

Business risk must be classified, evaluated for likelihood of occurrence, and estimated for potential impact in order to implement effective ERM. The Office of Management and Budget defines enterprise risk management as "an effective agency-wide approach to addressing the full spectrum of the organization's significant risks by understanding the combined impact of risks as an interrelated portfolio".

Enterprises face many different types of risks, and cyber security risk is only one of them. Many different kinds of risks, such as compliance, cybersecurity ("cyber information security"), financial, legal, legislative, operational, reputational, and strategic, are defined in Appendix A of Playbook: Enterprise Risk Management for the U.S. Federal Government. Safety, privacy, and supply chain risk management are just a few more areas that may be added to this list that have their roots in enterprise risk management (ERM). In ERM, businesses manage all of the risks they face as a whole.

Enterprise risk management (ERM) is defined by the COSO publication Enterprise Risk Management - Integrating with Strategy and Performance as the "culture, capabilities, and practices that organizations integrate with strategy-setting and apply when they carry out that strategy, with a purpose of managing risk in creating, preserving, and realizing value". The basic goal of ERM in both public and private organizations is to protect the organization's mission, finances (including net revenue, capital, and free cash flow), and reputation (including stakeholder trust) against unintended, unintentional, and malicious events.

This is done by weighing the potential consequences of various business risks on the accomplishment of the organization's long-term goals and objectives, as detailed in its strategic plan. Strategic, operational (operational effectiveness and efficiency), reporting (reporting reliability), and compliance (compliance with relevant laws and regulations) goals must be included in ERM risk profiles in accordance with OMB Circular A123. While there is likely some risk overlaps across the categories of objectives, knowing how uncertainty impacts these goals can aid in making good choices at the right moment. In this way, subordinate levels might get risk advice from higher levels thanks to context and classification procedures. The key to efficient ERM is striking a balance between safety goals and the best use of available resources. An organization's management is only as good as its ability to strike a balance between maximizing limited resources and minimizing risk.

Incorporating culture, strategy, and performance into ERM is a central theme of this paper. One such concept is that a company "must manage risk to strategy and business objectives in relation to its risk appetite". Risk appetite refers to the generalized kinds and levels of risk that a company is ready to take in order to maximize its value creation. Risk appetite "is the broad-based amount of risk an organization is willing to accept in pursuit of its mission/vision," as OMB rephrased it for government usage in Circular A-123. Decisions like strategy formulation and goal selection are governed by the enterprise's risk appetite, which is decided by the highest level of management.

Shortcomings of Typical Approaches to Cybersecurity Risk Management

The ERM framework and CSRM share many of the same high-level ideas. On the other hand, CSRM is seldom carried out in the same way, and its results are rarely conditioned enough to be used as inputs to ERM. The following are examples of frequent causes of such defects. Organizational risk communication, management, and integration may all benefit from the enterprise-based CSRM approach outlined in this study and the forthcoming volumes in this series.

Lack of Standardized Measures

The topic of how to evaluate cyber threats has been studied for decades. The measurement issue has become increasingly difficult to tackle

as both measuring tools and digital asset complexity have advanced. Standardization has been achieved at the lower levels of measurement, for example in the anticipated probability and effect of a given vulnerability being exploited. However, there are no universally accepted metrics for other forms of cybersecurity risk. There isn't a solid foundation for measuring risk or presenting risk consistently across digital assets and the systems comprised of those assets without uniform measurements.

Informal Analysis Methods

Inconsistencies in risk analysis are more common for CSRM than for many other types of risk. Even when guidelines are available, like NIST SP 800-30, there is a wide range of interpretations in the ensuing Risk Assessment Reports (RARs)15. In addition, there is often not a defined approach or basic inputs for probability and effect estimates are left to the discretion of suppliers that supply a grading system. Individuals often rely on their intuition and familiarity with common information and practices when making important decisions. Many security measures, for instance, are deployed automatically to safeguard a new device without previously determining the extent to which they would increase or decrease risk. Furthermore, when controls have been implemented, there is often minimal analysis undertaken to see whether risks have been decreased to an acceptable level (i.e., within the predetermined risk tolerance levels).

Focus on the System Level

many approaches used to managing cybersecurity risk at the system, organization, and enterprise levels. Individual teams inside a system are often tasked with monitoring potential threats. While it is possible for systems to report up to the organizational level, there is generally no method in place to integrate cybersecurity risk data at either the organizational or enterprise level. Often, the system cybersecurity risk data received by an organization or corporation is a constantly red heatmap or of an impractical amount. It's hardly unexpected that upper management has difficulty grasping the gravity of the threat posed by cyberspace. In businesses whose systems are mapped to the business processes they support; this may be less of an issue. Despite the fact that many corporate risks are interrelated, this article only addresses cybersecurity threats and how they relate to ERM. A prominent example is the possibility that a credit downgrade or a loss of public trust might arise from a cybersecurity compromise, even though these risks are distinct components of the ERM portfolio. Because of these interconnections, it is crucial for business leaders to work together, share information, and understand that threats to the company's data, infrastructure, and operations are all interconnected.

Increasing System and Ecosystem Complexity

It's very uncommon for the systems that agencies and other institutions rely on to be adaptive "systems of-systems" with thousands of moving parts and communication pathways. The systems function in a sociopolitical-technological setting that is in a constant state of flux, rife with danger from persons and organizations whose alliances, views, and ambitions are constantly altering.

Cyberspace has evolved and become more complex as a result of the ongoing introduction of new technology. New complications and risks have emerged as a result of the proliferation of wireless connectivity, big data, the cloud, and the Internet of Things. The information and technology landscape has evolved beyond a streamlined digital archive. They are more like to the brain, or central nervous system, of a company or organization, coordinating and controlling the most essential resources. The growing complexity of this ecosystem creates systemic risks and exploitable vulnerabilities that, if activated, may have a domino effect with various, catastrophic effects for businesses and the nation as a whole. Due to the ever-changing nature of natural ecosystems, securing them is a significant challenge.

The risks associated with these systems are amplified by the aforementioned complexity, and this in turn may result in more risks at the system, organization, and enterprise levels. It is also important to recognize, monitor, and

control the risks associated with the interdependence of systems and counterparty risk.

Cybersecurity Management

Management of cyber security is a subfield of information technology concerned with keeping private data safe from hackers and other intruders. One definition of Cybersecurity Management is provided below. One aspect of this is preventing data breaches of any kind, including those caused by cyber assaults, cyber threats, network intrusions, malware, and the like on the company's computer systems and networks.

The goal of cybercriminals is to locate and use whatever weakness in a system they can. And, sadly, they are becoming more and more sophisticated in their cyberattack methods. The population of cybercriminals is expanding as well. Some of them may even wreck a person's private computer system. However, businesses and other institutions are increasingly reevaluating their strategies for countering such threats. Now more than ever, companies and organizations are realizing the necessity of cyber security and taking steps to protect their data from hackers by employing managers and specialists in the field.

An organization's strategic deployment and execution of cyber security is the primary emphasis of an MSc in Cyber Security Management. Our mission is to foster the next generation of strategic thinkers who will be able to help any firm reach its full potential by analyzing problems, developing creative solutions, and articulating those ideas clearly to upper-level management.

Protecting your virtual territory is difficult since it calls for both technical knowledge on how to keep your digital systems and devices safe and effective human management. From swaying the risk tolerance of the board to overseeing firewall reconfiguration during a cyber-attack, we will teach you all you need to know to manage cyber security inside an organization.

Those with a background in consulting, strategy, business, or management may find this course particularly useful. Throughout the year, you'll get a thorough comprehension of the cyber threat environment and the potential progression of a cyber event. You will learn about the essential technologies used to safeguard an organization's information infrastructure from intrusion, as well as how to mitigate the effects of an attack should one occur.

IT systems in today's businesses are notoriously complex. Employees may use the on-premises and cloud services that make up the conventional IT stack from anywhere, not just the workplace. Because of this complexity, businesses are exposed to fresh threats to their data security and may face new avenues of attack from hackers.

Conclusion

The conceptual development of cyber security and risk management underscores the critical importance of addressing the complex and ever-evolving landscape of digital threats. As technology continues to advance, organizations and individuals alike find themselves increasingly reliant on interconnected systems, making the understanding and implementation of effective cyber security measures a fundamental necessity.The synergy between cyber security and risk management emerges as a strategic imperative, as organizations acknowledge that the scope and severity of cyber threats can disrupt operations, compromise sensitive data, and undermine trust. The holistic approach to security necessitates not only technological safeguards but also a deep comprehension of potential vulnerabilities, threat vectors, and the human element in risk mitigation.

Embracing the conceptual foundation of cyber security involves recognizing the dynamic nature of threats. As cyber adversaries adapt and exploit new vulnerabilities, proactive strategies that span prevention, detection, response, and recovery are essential. An integrated approach, informed by risk management principles, ensures that security investments are aligned with an organization's unique risk profile and strategic objectives.

The landscape of cyber security and risk management requires continual adaptation, anticipation of emerging threats, and the

incorporation of best practices. The conceptual development serves as the compass guiding organizations towards resilient and adaptable cyber security architectures, capable of mitigating risks while fostering innovation.

References

1. Liem, christina. (2018). Enterprise risk management in banking industry. Firm journal of management studies. 3. 1. 10.33021/firm. v3i1.381.
2. Erin, olayinka&emoarehi, eriki&arumona, jonah&jacob, ame. (2017). Enterprise risk management and financial performance: evidence from emerging market. International journal of management, accounting and economics. 4. 937-952.
3. Wu, desheng&olson, david. (2015). Enterprise risk management in finance. 10.1057/9781137466297.
4. Gazal, taiwohassan&olabisi, jayeola&kajola, sunday&olukayode, ezekiel. (2022). Enterprise risk management and financial sustainability: evidence from nigerian listed consumer goods firms. 22. 20.
5. Soliman, alaa&adam, mukhtar. (2017). Enterprise risk management and firm performance: an integrated model for the banking sector. Banks and bank systems. 12. 116-123. 10.21511/bbs.12(2).2017.12.
6. Khan, mohammedabdulimran&alkathiri, mohamed&alhaddad, hamid&alnajjar, faisal. (2021). Impact of erm on sustainability and financial performance of enterprises in the gulf cooperation council: case study of oman. International journal of management. 12. 598-609. 10.34218/ijm.12.1.2021.051.
7. Andronache, alina&althonayan, abrahim. (2019). Resiliency under strategic foresight: the effects of cybersecurity management and enterprise risk management alignment. 10.1109/cybersa.2019.8899445.
8. Cox, louis &popken, douglas& sun, richard. (2018). Causal analytics and risk analytics. 10.1007/978-3-319-78242-3_1.
9. Wang, wei&cammi, antonio& di maio, francesco&lorenzi, stefano&zio, enrico. (2018). A monte carlo-based exploration framework for identifying components vulnerable to cyber threats in nuclear power plants. Reliability engineering & system safety. 175. 10.1016/j.ress.2018.03.005.
10. Krisper, michael&dobaj, jürgen& macher, georg&schmittner, christoph. (2019). Riskee: a risk-tree based method for assessing risk in cyber security. 10.1007/978-3-030-28005-5_4.
11. Burenok, d &cherniaev, v. (2021). Monte carlo method for solving the problem of predicting the computer network resistance against dos attacks. Journal of physics: conference series. 2099. 012069. 10.1088/1742-6596/2099/1/012069.
12. Constante flores, gonzalo&illindala, mahesh. (2019). Data-driven probabilistic power flow analysis for a distribution system with renewable energy sources using monte carlo simulation. Ieee transactions on industry applications. 55. 174 - 181. 10.1109/tia.2018.2867332.
13. Finke, gandolf&singh, mahender&rachev, svetlozar. (2010). Operational risk quantification–a risk flow approach. Journal of operational risk. 5. 10.21314/jop.2010.083.
14. Sion, laurens&yskout, koen&landuyt, dimitri&joosen, wouter. (2018). Risk-based design security analysis. 11-18. 10.1145/3194707.3194710.
15. Alhomidi, mohammed& reed, martin. (2014). Attack graph-based risk assessment and optimisation approach. International journal of network security & its applications. 6. 31-43. 10.5121/ijnsa.2014.6303.