Cybersecurity Risk Management

Amjad Alqahtani
dept. of computer science
Univeristy of Texas at San Antonio
San Antonio, Texas, USA
amjad.alqahtani@my.utsa.edu

Abstract—**This document discusses cybersecurity risk management as a requirement for organizations in the interconnected digital world. Risk-based and maturity-based methodologies are the primary cybersec risk management protocols applied. This paper will cover what they entail, their historical context, their applications, evaluate the best approach, and recommend the best protocol for SMBs before concluding.**

Keywords—Cybersecurity, risk management, risk-based approach, Maturity-level approach, organizations

I. Introduction

Organizations face relentless cyber threats in an increasingly interconnected digital landscape, driving the need for effective risk management strategies. There are two predominant methodologies for achieving cybersecurity resilience: risk-based and maturity level. The risk-based approach seeks to identify, prioritize, and mitigate the threats based on risk appetite by dynamically deploying resources to high risks. In contrast, the maturity level approach encourages the gradual maturity of cybersecurity processes from predefined maturity levels. Although this method is suitable for systematic, long-term capability building, it may not be able to respond promptly to immediate risks. However, these approaches can complement each other despite frequently being characterized as opposite paradigms. Maturity models improve foundation controls and institutionalize best practices, whereas a risk-based strategy enables rapid response to well-identified critical threats. Theoretical foundations, practical trade-offs, and contexts in which one excels are identified for each model. This case study analyzes and investigates a hybrid framework and suggests a healthy balance between adaptive risk prioritization and a structured maturity progression.

II. Understanding Risk-Based and Maturity-Level Approaches

The risk-based approach is a dynamic risk management tactic that seeks to identify, measure, and evaluate the risk an organization is exposed to and manage it effectively. The most critical threats are mapped to replace broad, standardized safety measures with the likelihood and impact addressed [1]. Its purpose is to channel the resources to address the foremost risks efficiently. However, this approach means the threat landscape changes with time since technological advancement, emerging cyber threats, and regulatory changes are always evolving [2]. Organizations are undertaking a much more effective form of asset security by adopting a risk-based approach based on security measures aimed at critical vulnerabilities.

One example is a financial institution that chooses to put more effort into protecting its customers' data and transaction systems from cyberattacks. Alternatively, a manufacturing company can focus on ensuring that its supply chain is not disrupted [3]. The risk-based approach offers so much flexibility and adaptability that it is most effective for organizations operating in dynamic environments where new risks keep emerging. Nevertheless, implementing this strategy entails carrying out proactive risk identification and ongoing monitoring in real-time, which consumes resources.

On the other hand, the maturity-level (maturity–based) approach evaluates an organization's risk management capabilities through a structured framework. This method classifies the organization’s risk exposure into different maturity stages, from the initial stage, where risk management is unstructured and reactive, to the optimal stage, where risk management is fully incorporated into the organization's processes and improved incrementally [2]. No formal policies exist at lower maturity level organizations, where either reactive or no strategies are adopted. In comparison, higher maturity-level entities have defined proactive security measures and utilize automation and data-based effective decision-making.

A maturity-based approach improves cybersecurity posture by progressively moving organizations through maturity levels related to their cybersecurity posture. Frameworks such as the NIST CSF, CMMI, and the standardized ISO 27001 [4] provide the steps and criteria for adopting and implementing the risk management process by various parts of the organization. Following these models, organizations can improve their resilience and increase compliance and the risk governance level.

The main difference between the two approaches is what they target. The risk-based approach is real-time and addresses the most pressing risks. However, a maturity-based approach is process-oriented and developmental, focusing on the long–term capabilities of a firm’s risk management and suggesting a structured improvement process [2]. Few organizations use both approaches to create a well-balanced and effective risk management strategy. To mitigate the immediate threats, they use a risk-based approach, while the overall security framework is strengthened step by step by following a maturity-based approach [4]. Thus, a hybrid approach using both methods guarantees short-term and long-term protection against evolving risks.

III. Risk Management Historical Context

Organizations have always relied on a risk-based approach, allowing them to identify and mitigate threats. This method was particularly effective in industries where immediate risk response was crucial, such as finance, healthcare, and defense [5]. Early cybersecurity frameworks focused on detecting, analyzing, and countering active threats, ensuring organizations could protect sensitive data and critical infrastructure from breaches, fraud, and cyberattacks.

In the financial sector, for instance, banks and payment processors implemented real-time fraud detection systems to combat cyber threats as they emerged. Similarly, governments and military organizations developed sophisticated cybersecurity measures in the defense sector to counteract espionage, cyber warfare, and data breaches [6]. Because these sectors handled highly sensitive and mission-critical data, a risk-based approach allowed them to respond rapidly to vulnerabilities before they could be exploited [5]. However, this approach may aid in mitigating immediate threats, but there is no clear way to improve security practices in the long term.

As organizations increasingly rely on digital infrastructure and threats become more complex, a long-term and structured security improvement is required. A maturity-based approach to gradually enhancing risk management capability in such a situation becomes necessary [1]. In the 1990s and 2000s, risk maturity models (RMM), CMMI, and later the CSF made maturity models popular [4], [7]. Organizations adopted structured pathways to evaluate, enhance, and develop risk management practices over time.

One key advantage of a maturity-based approach is that it is systematic. This approach takes organizations through different maturity levels, from ad hoc and reactive processes to optimized and continually improving security [3], [4]. A maturity-based approach is unlike a risk-based approach focused on individual risk, as this approach enables organizations to build resilience by improving their overall cybersecurity posture.

Both approaches are currently used based on an organization's needs, but an increased focus is on the maturity-based approach. This is a consequence of the evolving cybersecurity landscape, which leads to bigger and more sophisticated threats [6]. For example, compliance with regulatory requirements such as GDPR, HIPAA, and ISO 27001 is imperative for modern organizations as they must actively take proactive a security approach to tackling security challenges [8]. However, cyber threats such as ransomware, supplier chain attacks, and zero-day exploits call for adjusting to long-term protection models as a substitute for short-term reactive measures.

Contemporary cybersecurity risk management structures combine risk-based and maturity-based approaches, offering different qualities that many organizations want. The organizations use a risk-based approach to fight perceived immediate threats and apply a maturity-based framework to improve resilience, compliance, and security governance [3]. This hybrid strategy ensures companies are ready for current threats and improves their defense against future risks.

IV. IV INDUSTRY-SPECIFIC APPLICATIONS

From the operational point of view, different industries adopt risk-based and maturity-based approaches to cybersecurity. This depends upon the nature of the business, its operational necessity, the regulatory compliance requirements it is subject to, and the threat environment under consideration. In some industries, threat mitigation must take place immediately. To that end, a risk-based approach is more suitable, whereas others stress long-term security improvements, thus a maturity-based approach.

Mobile banking, digital payments, and financial transactions rely on a risk-based approach, and the financial sector relies on it heavily. The financial industry is constantly under cyber threat, which includes fraud, phishing, malware, identity theft, and account takeovers [5]. With risks changing rapidly, it is important to identify and deal with them in real-time. For instance, banks instill real-time fraud detection systems that use machine learning (ML) and artificial intelligence (AI) to detect transaction patterns [6]. When an unusual transaction takes place, the system immediately sends it out for review to prevent the possibility of a financial loss. Also, multi-factor authentication (MFA) and transaction encryption are the priorities for immediate security steps that prevent customer accounts from succumbing to threat actors. Although a risk-based approach is the standard approach for financial services, some maturity-based risk management is also required by regulatory requirements like Basel III, PCI-DSS, and GDPR [8], [9]. To stay compliant and trusted by the customers, banks and financial institutions must simultaneously work on immediate threat response and long-term cybersecurity improvement.

Maturity-based models are mainly adopted by industries such as healthcare, critical infrastructure (energy, transportation, and telecommunications), and government agencies, where strict regulatory requirements are mandatory. These are important industries that deal with sensitive personal, national, and operational data regularly and, therefore, require a structured security framework that must be put into place and followed for a long time to ensure it is legal and ethical. For example, HIPAA (Health Insurance Portability and Accountability Act) requires that all patient data be protected in healthcare organizations [8]. By taking a maturity-based approach, hospitals and clinics put in place a process whereby cybersecurity controls mature, secure access management is implemented, and regular risk assessments are performed.

Moreover, CSF must be complied with by the critical infrastructure sectors. Each must pass through different maturity levels to enhance their cyber security measures to avoid attacks on power grids, water supply, and communication networks. Government agencies also tend to follow standards like ISO 27001 to create a structured approach to risk management. On the other hand, it becomes relatively impossible for it to move on with its cybersecurity practices in a reactive manner [8]. These industries can develop long-term resilience against cyber threats by adopting a maturity-based approach and minimizing the exposure before they are exploited rather than reacting after an attack.

Startups and most technology-driven companies, especially in software development, e-commerce, and cloud computing, prefer a risk-based approach since they need to be agile. Unlike big business, startups have limited budgets to enforce the complete set of cybersecurity maturity models [3], [4]. They aim to tackle short-term threats such as data breaches in a cloud environment, DDoS (Distributed Denial of Service) attacks on web applications, and API vulnerability in software integration that may affect their operation [6]. For example, a SaaS (Software as a Service) startup may invest more in end-to-end encryption and cloud security monitoring of its customer database rather than build a maturity framework [4]. However, as startups grow, they tend to include maturity-based frameworks, such as ISO 27001 certification, to gain the trust of investors and clients.

Thus, industry requirements, regulatory obligations, and resource availability are the deciding factors when choosing risk-based or maturity-based approaches. Financial services and technology startups prioritize immediate threat mitigation through a risk-based approach. On the other hand, regulated industries such as healthcare, critical infrastructure, and government emphasize long-term cybersecurity improvements using maturity-based frameworks. Many organizations adopt a hybrid approach, combining real-time risk management with structured, long-term security enhancements to ensure short-term protection and long-term resilience.

V. Best Approach Evaluation

To determine the best cybersecurity strategy, neither a risk-based nor a maturity-based approach should be considered better. Both have a separate purpose that distinguishes each one apart from the other. There is no best choice since what is best depends upon an organization's size, industry, regulatory environment, and the particular security problems that the organization faces.

A risk-based approach is best for organizations that operate in fast-paced, high-risk, high-evolving cyber threats. This approach aims to find, measure, and combat the greatest security risks in terms of probability and consequence [10]. The risk-based approach is helpful to Financial Institutions, Tech Startups, Retail, and e-commerce platforms. The advantages of this approach are flexibility and responsiveness [5]. It helps security teams prioritize and allocate resources to the highest critical vulnerabilities. However, its reactive nature may poke holes in long-term cybersecurity planning, making organizations susceptible to emerging threats that are not quickly prioritized.

Organizations that need long-term, systematic improvements in security and must follow strict regulatory compliance will find a maturity-based approach more suitable. This approach helps organizations gradually enhance cybersecurity by improving policies, procedures, and controls over time [1]. Healthcare organizations, critical infrastructure sectors, and government agencies are the industries that benefit most from a maturity-based strategy. The most significant advantage of a maturity-based approach is its proactive and structured nature, which helps organizations build cybersecurity resilience and ensure compliance with industry regulations [11]. However, this approach may lack agility, making it difficult to address urgent threats in real-time without additional risk-based mechanisms.

While each framework is stand-alone, a hybrid approach that combines the best of both strategies is advisable. Both approaches offer unique benefits such that many organizations find a hybrid model the most effective strategy [12]. Integrating risk-based decision-making with a maturity-based framework enables organizations to address immediate security threats based on a risk-based approach and apply the maturity-based approach to develop long-term security improvements [13]. This ultimately helps the organization comply with the industry regulations and adapt to newer risks.

VI. VI RECOMMENDATION FOR SMALL-TO-MEDIUM-SIZED BUSINESSES (SMBS)

A risk-based approach is the most practical starting point for both startups and SMBs with few cyber security resources. Some of the challenges these organizations face include budget constraints, small IT teams, and the need to operate quickly [14], making it difficult for them to apply a comprehensive and maturity-based cybersecurity framework from the outset. Thus, by giving precedence to imminent threats and implementing cost-effective security measures, they can secure their sensitive assets without incurring enormous overheads.

Startups and SMBs can use a risk-based approach to identify and protect against the top threats to an organization, including phishing, malware, and data breaches. The second advantage is that it allows them to utilize their resources more efficiently by first addressing critical threats [3]. In addition, firewalls, endpoint protection, MFA, and regularly updating software will not bankrupt small businesses but will help improve security.

However, as the business grows, it takes in more customers, sensitive data, and more regulations, so a risk-based approach may not be enough. A maturity-based model is of the essence at this stage. Businesses can follow up with established cybersecurity policies and governance as they mature to meet regulatory requirements such as GDPR, SOC 2, and ISO 27001 [8] and secure long-term cybersecurity resilience. Introducing maturity-based security practices such as regular security training, incident response planning, and proactive risk assessments can greatly improve cybersecurity posture with the startups and small businesses in an advanced status. The hybrid approach provides immediate protection and a long-term increase of security that is aligned with industry best practices and is flexible to business needs.

CONCLUSION

Risk-based and maturity-based approaches are necessary to secure organizations as they have benefits that fit organizational requirements. Most security benefits are derived from organizations that follow a risk-based approach to take care of threats that require quick action. Superior cybersecurity resilience is achieved with a structured approach, which is implemented with a long-term plan through a maturity-based approach. Therefore, it is possible to apply a durable security framework that evolves with threats and has standardized policies and continuous improvement processes. For SMBs, the best initiation point is the risk-based approach since it is the most practical and affordable way to protect their systems. Initial risk mitigation of urgent security challenges can enable SMBs to continue to operate and stay flexible. Businesses should implement maturity-based elements as they grow to ensure that they continue to have proper cybersecurity effectiveness with limited resources. Modern business protection requires a combination of risk-based and maturity-based approaches to counter present dangers and construct enduring cybersecurity risk management platforms.

References

[1] L. Utami and R. D. Pasaribu, "Effectiveness of Risk Management through Risk Maturity Measurement: A Study at PT Pelabuhan Indonesia," *International Journal of Science Technology & Management*, vol. 5, no. 4, pp. 970–984, Jul. 2024, doi: 10.46729/ijstm.v5i4.1158.

[2] M. Wieczorek-Kosmala, "Risk management practices from risk maturity models perspective," *Journal of East European Management Studies*, vol. 19, no. 2, pp. 133–159, Jan. 2014, doi: 10.5771/0949-6181-2014-2-133.

[3] eSentire, “Maturity-based approach vs. Risk-Based approach: What’s the right answer?,” *Cyber Defense Magazine*, Aug. 09, 2021. https://www.cyberdefensemagazine.com/maturity-based-approach

[4] A. Buzdugan and G. Căpăţână, “The trends in Cybersecurity maturity models,” in *Smart innovation, systems and technologies*, 2023, pp. 217–228. doi: 10.1007/978-981-19-6755-9_18.

[5] M. C. Scheau, L. Gabudeanu, L. Apetri, and C. N. Bodescu, “Risk-based approach in preventing mobile banking cyber-attacks.,” *25th RSEP International Conference on Economics, Finance & Business*, Art. no. 978-605-70583–8–6, doi: 10.19275/RSEPCONFERENCES174.

[6] U. Islam *et al.*, “Detection of distributed denial of service (DDOS) attacks in IOT based monitoring system of banking sector using machine learning models,” *Sustainability*, vol. 14, no. 14, p. 8374, Jul. 2022, doi: 10.3390/su14148374.

[7] S. R. Treadwell, “Using critical incidents to explore the lived experiences of information security executives - ProQuest.” https://www.proquest.com/openview/5f9e9bc1cb7dd3bbf050a82d6ecc5c92/1?pq-origsite=gscholar&cbl=18750&diss=y

[8] J. Nowicka, Z. Ciekanowski, and A. Milewska, “Information security management as the basis for the functioning of an organization,” 2024. https://www.um.edu.mt/library/oar/handle/123456789/127249

[9] C. S. Seah, Y. X. Loh, M. Falahat, W. S. Loh, and A. N. A. Nuar, “Guardians of Trust: Fortifying Payment Gateway Security for Digital Prosperity,” in *Emerald Publishing Limited eBooks*, 2024, pp. 43–58. doi: 10.1108/978-1-83608-634-520241006.

[10] I. Lee, “Cybersecurity: Risk management framework and investment cost analysis,” *Business Horizons*, vol. 64, no. 5, pp. 659–671, Feb. 2021, doi: 10.1016/j.bushor.2021.02.022.

[11] H. I. Kure, S. Islam, and H. Mouratidis, “An integrated cyber security risk management framework and risk predication for the critical infrastructure protection,” *Neural Computing and Applications*, vol. 34, no. 18, pp. 15241–15271, Feb. 2022, doi: 10.1007/s00521-022-06959-2.

[12] M. Gale, I. Bongiovanni, and S. Slapnicar, “Governing cybersecurity from the boardroom: Challenges, drivers, and ways ahead,” *Computers & Security*, vol. 121, p. 102840, Jul. 2022, doi: 10.1016/j.cose.2022.102840.

[13] U. Lagap and S. Ghaffarian, “Digital post-disaster risk management twinning: A review and improved conceptual framework,” *International Journal of Disaster Risk Reduction*, vol. 110, p. 104629, Jun. 2024, doi: 10.1016/j.ijdrr.2024.104629.

[14] M. N. Y. Marican, S. A. Razak, A. Selamat, and S. H. Othman, “Cyber Security Maturity Assessment Framework for Technology Startups: A Systematic Literature Review,” *IEEE Access*, vol. 11, pp. 5442–5452, Dec. 2022, doi: 10.1109/access.2022.3229766.