International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

An Analysis of Cyber Threat in the Merger and Acquisition Process and the Role of Cyber-security for a Successful Merger

Dr. Neeti Pandey[1], Kamal Kishore Rajoriya[2]

[1]LL.M. Ph.D. Law, Principal, Madhav Vidhi Mahavidhalaya, Gwalior.
[2]LL.M. 2nd Semester, Research scholar, Madhav Vidhi Mahavidhalaya, Gwalior

Abstract
Businesses are increasingly giving cybersecurity the attention it deserves to facilitate successful mergers and acquisitions. Cyber security due diligence is not only essential for just the acquiring company. Excellent cybersecurity benefits both sides of the M&A process. A clean bill of health concerning cybersecurity can make a target firm more attractive, and cybersecurity best practices on both ends make for a smoother, more secure transition period. This Research paper analysis the major cyber threat possible in Merger and Acquisition cases and provide deep understanding of the cyber risk in merger deals, the role of due diligence in Cyber Security and migration strategies for Cyber Risk in merger. This paper concludes that cybersecurity is a critical consideration in the M&A process, with data breaches and cyber threats posing significant risks to both acquiring and target companies. By adopting a proactive and multi-layered approach to cybersecurity, businesses can mitigate risks, protect sensitive data, and foster a smooth post-merger integration. Prioritizing cybersecurity throughout the M&A lifecycle is essential in today's digital landscape to safeguard against evolving cyber threats.

I. Introduction

Businesses are increasingly giving cybersecurity the attention it deserves to facilitate successful mergers and acquisitions. In the current threat landscape, cybersecurity concerns, such as discovering an unreported data breach, are enough to cause deals to fall through. M&A activity necessitates strong cybersecurity policies, audits, and measures to identify, remediate, and mitigate the target business's security problems and vulnerabilities.

However, cybersecurity due diligence is not only essential for just the acquiring company. Excellent cybersecurity benefits both sides of the M&A process. A clean bill of health concerning cybersecurity can make a target firm more attractive, and cybersecurity best practices on both ends make for a smoother, more secure transition period.

II. Understanding Cyber Threats In Merger Deals:

In today's digital age, the escalating complexity and frequency of cyber threats have elevated the significance of cybersecurity. Cybercriminals employ sophisticated tactics like ransomware, phishing, and data breaches to target individuals, businesses, and even governments. The expanding attack surface

poses a significant challenge in cybersecurity. The proliferation of IoT devices, cloud computing, and mobile devices has increased the number of entry points for cybercriminals to exploit. With billions of smartphones and IoT device users globally, organizations must proactively monitor and secure interconnected devices and systems to address this concern.

The evolving cyber threat landscape is characterized by highly targeted and advanced threats, including ransomware, APTs, and zero-day vulnerabilities. Traditional antivirus software alone is no longer sufficient to combat these threats. A multi-layered approach that includes advanced threat detection technologies, behavioural analytics, and real-time threat intelligence is necessary for effective cybersecurity. Nation-state-sponsored attacks have emerged as another critical challenge. Governments use cyber espionage and warfare for political and economic advantage, posing severe implications for national security. To tackle the evolving cyber threats, harnessing technology is crucial. Machine learning and artificial intelligence enhance cybersecurity capabilities by analysing vast amounts of data to identify potential threats.

However, technology alone cannot ensure cybersecurity. It requires a shared responsibility involving individuals, businesses, and governments. Educating individuals about risks and best practices is vital to protect themselves online. For businesses, prioritizing cybersecurity, implementing strong access controls, and conducting regular vulnerability assessments are essential measures. Governments must enact and enforce robust cybersecurity regulations to foster collaboration, information sharing, and accountability in the digital ecosystem.

The dynamic nature of cyber threats necessitates a proactive and comprehensive approach to cybersecurity. Continuously updating systems, staying informed about the latest threats, and investing in advanced defence mechanisms are essential to safeguard the interconnected world we live in today. Cybersecurity is no longer a luxury but a necessity in ensuring a secure digital environment for all stakeholders.

III. Role Of Due Diligence In Cyber Security:

The process of mergers and acquisitions (M&A) introduces critical cybersecurity risks that can jeopardize negotiations and have far-reaching consequences for both the acquiring and target companies. Failure to address these issues not only exposes the original business to potential threats but also impacts its supply chain. The cost and time required to rectify severe cybersecurity issues may even threaten the successful completion of the deal.

- **Technological Integration:**

A Key Risk Factor Merging companies often face challenges related to technological integration, particularly when upgrading technology during the process. Full hybrid integration, which involves integrating new technologies with legacy systems, presents compatibility and scaling issues. Unfortunately, this disruption can create a favourable environment for cyber attackers to execute their malicious activities. Unusual cyber activities may go unnoticed amid the technological chaos, leading to data breaches and unauthorized access.

- **Dormant Threats and IoT Risks:**

The acquired infrastructure may harbour dormant cybersecurity threats, such as undetected malware or access management issues. Moreover, the rise of Internet of Things (IoT) devices has complicated M&A cybersecurity efforts. Converging traditional IT with operational technology increases the attack surface, leaving companies vulnerable to cyberattacks. Auditors may overlook some IoT devices during security assessments, making them potential weak links in the overall cybersecurity posture.

- **IT Resiliency and Cyber Attacks:**

During the M&A process, extended periods of IT resource overburdening may occur as firms integrate their technologies. This heightened activity creates vulnerabilities that cybercriminals can exploit through phishing, ransomware, or Distributed Denial of Service (DDoS) attacks.

- **Data Security and Lack of Information:**

In the M&A process, two sets of critical data are at stake, demanding a thorough assessment of cybersecurity risks for both organizations. However, in cases of smaller acquisitions, the acquiring company may face challenges in obtaining adequate documentation on the target firm's cybersecurity policies and practices. This gap complicates the cybersecurity due diligence process and may expose the acquiring company to unforeseen cyber threats.

- **Organizational Disruption and Prioritizing Cybersecurity:**

The process of merging two organizations often leads to significant disruptions as new roles, responsibilities, and operational practices are established. Amidst these changes, maintaining stable information systems and cybersecurity becomes challenging. Companies with mature and advanced cybersecurity controls are better equipped to identify, manage, and mitigate M&A cybersecurity risks.

- **Cybersecurity Considerations Throughout the M&A Lifecycle:**

To navigate the M&A process successfully, both the acquiring and target firms must adopt a collaborative approach. Governance, policies, managerial processes, tools and technology, and risk metrics should be well-defined and aligned to ensure effective cyber risk management. Risk assessments and threat hunting activities should continue throughout the integration process to identify and remediate vulnerabilities promptly.

With the increasing complexity of M&A activities in today's business landscape, cybersecurity must be at the forefront of strategic planning. From the initial stages of due diligence to post-integration operations, companies must prioritize cybersecurity efforts to safeguard sensitive data and protect against cyber threats. By emphasizing on cybersecurity, businesses can navigate the intricate M&A landscape with confidence and resilience.

III. Mitigation Strategies For Cyber Risks In Mergers

The article highlights the significant cybersecurity risks associated with mergers and acquisitions (M&A) and provides five key strategies to manage these risks effectively. It emphasizes the importance of considering cybersecurity early in the M&A process to avoid potential pitfalls that may lead to buyer's remorse or costly post-merger remediation efforts.

- **Security Assessment of the Target Firm:**

Conducting a thorough security assessment of the target company before acquisition is crucial. By evaluating the target company's security posture and policies, the acquiring organization can determine whether they align with its strategic goals and risk appetite. Moreover, acquiring companies should be informed of any past security incidents, whether or not they were legally required to be disclosed, to gain a comprehensive understanding of potential risks.

- **Software Security Integration:**

In technology-focused mergers, cybersecurity becomes a major consideration. Acquiring companies must assess whether the target company has designed security into its software products. Failure to do so may lead to unexpected future remediation work and heightened chances of data breaches. In such cases, buyers may negotiate valuation adjustments or set aside funds in escrow to address potential security issues. A careful evaluation of the target's software security is essential to prevent any unpleasant surprises after the merger.

- **Early Involvement of Cybersecurity and IT Teams:**

The involvement of cybersecurity and IT teams in the early stages of M&A is essential to identify potential weaknesses and vulnerabilities. In some cases, target companies may lack even basic security measures, which could result in significant costs for remediation. Having these teams participate in the due diligence process ensures a structured approach to onboarding new acquisitions, including immediate security assessments and appropriate training for employees.

- **Understanding Data Environment Risk:**

Acquiring organizations must conduct a thorough analysis of the data environment of the target company. This analysis includes understanding the types of data involved (e.g., personal information, healthcare information, payment data) and the applicable regulatory requirements. Failure to comprehend the risks associated with the data environment may lead to an incomplete understanding of the target company's security controls and overall security posture.

- **Skills Analysis of Target Company's Employees:**

Beyond technology, acquiring companies also inherit the target company's employees. A skills analysis is necessary to assess if the acquired staff can meet the demands of the integration process. Overlooking skill gaps and not adequately supporting the staff during integration can lead to burnout, low morale, and an increase in cybersecurity vulnerabilities.Top of FormData breaches during mergers and acquisitions pose significant risks, exposing confidential corporate information to hackers. High-profile cases like Yahoo's acquisition by Verizon, where 500 million user accounts were compromised and Marriott's acquisition of Starwood Hotels, where 400 million guest records were exposed, highlight the severity of the issue. Such breaches not only lead to reputational damage but also legal consequences, as seen in Marriott's case, where they faced a $123 million GDPR fine. With the increasing frequency of data breaches in M&A, companies must prioritize cybersecurity and conduct thorough due diligence to mitigate these risks and safeguard sensitive data.

IV. Conclusion:

In conclusion, cybersecurity is a critical consideration in the M&A process, with data breaches and cyber threats posing significant risks to both acquiring and target companies. To ensure a successful and secure merger, organizations must prioritize cybersecurity through thorough due diligence, early involvement of cybersecurity teams, and proper evaluation of the target's security posture.By adopting a proactive and multi-layered approach to cybersecurity, businesses can mitigate risks, protect sensitive data, and foster a smooth post-merger integration. Prioritizing cybersecurity throughout the M&A lifecycle is essential in today's digital landscape to safeguard against evolving cyber threats.

References

1. https://www.upguard.com/blog/the-role-of-cybersecurity-in-mergers-and-acquisitions/
2. https://www.infosys.com/iki/perspectives/data-privacy-mergers-acquisitions.html
3. https://chambers.com/articles/cybersecurity-risks-in-ma-transactions
4. https://www2.deloitte.com/content/dam/Deloitte/us/Documents/mergers-acqisitions/us-ma-dont-drop-the-ball-Identify-and-reduce-cyber-risks-during-m-and-a.pdf
5. https://www.financierworldwide.com/cyber-hygiene-identifying-and-defusing-risks-in-ma
6. https://www.ey.com/en_in/strategy-transactions/cybersecurity