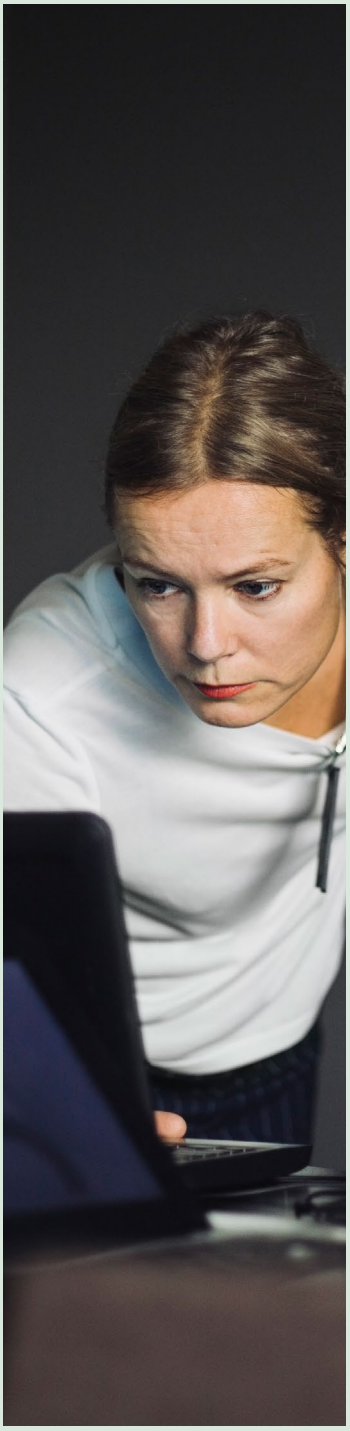
WHITE PAPER



CYBERSECURITY DUE DILIGENCE IN M&A: IDENTIFYING AND MITIGATING RISK BEFORE THE DEAL

Abstract

Cybersecurity risks are increasingly becoming a pivotal factor in Mergers and Acquisitions (M&A). As organizations grow through acquisitions, understanding and mitigating potential cyber threats is critical to ensure the success and longevity of the transaction. This whitepaper explores the importance of cybersecurity due diligence in M&A, outlining the challenges organizations face, the methodologies for identifying and mitigating risks, and best practices for executing effective cybersecurity evaluations. As per Forescout survey, 73% of respondents agreed that a company with an undisclosed data breach is an immediate deal breaker in their company's M&A strategy; whereas 53% of organizations have encountered a cybersecurity issue during M&A due diligence that jeopardized the deal.

Infosys®
Navigate your next

Why is Cybersecurity Due Diligence important from transaction perspective?

Cybersecurity-related risk and gaps can delay M&A transactions, impacting the overall timeline and potentially the financial value of the transaction. Delays can arise from the need to conduct thorough cybersecurity assessments, remediate identified risk and vulnerabilities, and adhere to regulatory requirements. These delays can lead to increased transaction costs, prolonged periods of uncertainty, and potential loss of competitive advantage.

More than half of all respondents (52%) report that a major undiscovered or undisclosed cybersecurity risk was revealed during the post-closing integration phase of their most recent deal. Therefore, by focusing on pre-transaction cybersecurity due diligence, M&A transactions can better safeguard their underlying operations from hidden or unknown vulnerabilities and risks in potential target companies.

Overview of Challenges and Industry Problem

The rise of cyber threats in an increasingly digital world has made cybersecurity a critical issue in M&A transactions. Inadequate due diligence can leave acquirers vulnerable to hidden risks, which may include exposure to outdated technology, unpatched vulnerabilities, data breaches, and third-party risks.

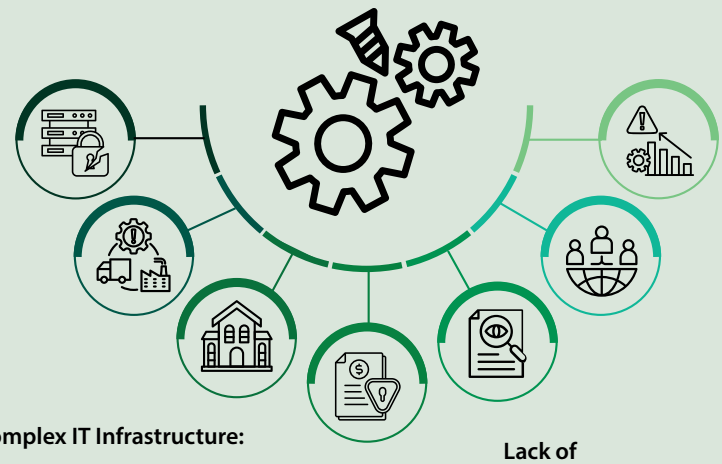
Undetected Data Breaches:

Data breaches occurring before an acquisition can remain undetected for extended periods. According to 2024 Cost of a Data Breach Report by IBM, the average time to identify and contain a breach is 292 days. Such delays can lead to significant liabilities post-acquisition.

Moreover, 73% of respondents agreed that a company with an undisclosed data breach is an immediate deal breaker in their company's M&A strategy.

Third-Party and Supply Chain Risks:

Many companies rely on third-party vendors, which can introduce vulnerabilities. As per AON Survey, Supply Chain or Distribution Failure is the sixth biggest risk facing organizations globally today.



Complex IT Infrastructure:

Merging different IT environments can create security gaps and complicate the integration process.

The model of private equity (PE) M&A differs from corporate M&A in several key aspects. Unlike corporate acquisitions, PE firms typically do not integrate the IT systems of their portfolio companies, therefore eliminating IT integration concerns. However, this lack of integration can result in heightened cyber risk. Each portfolio company retains its own cyber risk profile, but the associated costs, liabilities, and potential reputational damage can impact the PE firm, making cybersecurity a high priority.

Data Privacy Issues:

Different jurisdictions may have varying compliance requirements (GDPR, CCPA), adding complexity to data protection measures.

Lack of Transparency:

Many target companies may not fully disclose their cybersecurity posture, leaving acquirers unaware of critical vulnerabilities and risks.

The biggest challenge identified related to Cybersecurity due diligence during the survey conducted by Admincontrol and Mergermarket is "accurately vetting" the relevant information.

Increasing Regulations and Compliance:

Rising regulatory pressures, such as Digital Operational Resilience Act (DORA), Network and Information Systems Directive (NIS 2), and industry-specific requirements, require extensive compliance checks to avoid hefty fines.

Cultural Misalignment:

Mismatched approaches to cybersecurity policies and protocols between merging entities can slow down the integration process. As per survey conducted, over half of respondents (53%) report dedicating more resources to cybersecurity due diligence in their most recent deals compared to 12-24 months ago.

Fig 1. Key challenges in M&A transactions

Drivers & Motivation for M&A Service

Why carrying out a Cyber Security M&A due-diligence is important for an organization and a multitude of interconnected challenges it can help mitigate ?

Risk exposure throughout the M&A Lifecycle

Inadequate planning, reactive approach will impact the entity's risk posture over the course of M&A. Buyer could inherit risk and liabilities

Lack of People Cohesion

Without a clear RACI model for the merged entity, ambiguities and insecurities are likely to take a foothold thereby impacting risk posture

Lack of Technology-stack Cohesion

Disruptive vs Legacy solutions, Cloud vs On-prem vs Hybrid, Technology overlap, License overlap, Scaling security and integrating security in the target landscape

Limited assurance

Lack of documentation and supporting evidence regarding the cyber landscape for the target company is limited for the acquiring company to rely on

Data protection

Missing data protection practices at the could lead to liabilities in terms of regulatory compliance penalties and damaged reputation

Running against Time

Driven by business imperatives and without a Cyber Security roadmap, M&A phases will tend to outpace the Cyber security target operating model

M&A Anti-patterns

All is top priority, Ignoring or underestimating technical debt, Architectural anti-patterns impacting agility, resilience continuity

Importance & Business Value

"M&A Activity is a Top 5 Key Trigger for criminals to hack – individuals, groups or state funded to destroy and or ransom an organisations value prior, during or post-deal and thus Cybersecurity due diligence and risk assessment should and must be an ongoing activity"

Value to Buyer	Value to Seller
1 Identify Red Flags	1 Fix Material Risks
2 Understand True Cost	2 Confidence in Valuation
3 Negotiate better terms	3 Independent Evaluations
4 Stay Compliant	4 Achieve Compliance

Key Considerations

Primacy Factors

- **Cyber Incidents** – Exponential increase in the scale and impact of Cyber issues/problems and incidents – Short. Medium &Long Terms
- **Threat Landscape** – Business are more connected with more data, third parties, information sharing, cloud services – Risk Exposure
- **Compliance & Regulations** – Increasing penalties and fines for PII data exposure, prior and post M &A – Education & Awareness/ Ways of Working

Risk(s) Identification	• Identifying hidden risks, such as vulnerabilities, misconfigurations, data privacy non-compliance, cyber threats as part of day-to-day operations.
Value	• Valuing cyber risk for specific events such as theft of customer data or IP, or business disruptions/ outages and down time. Supports BMC/ DR Resilience.
Quantify	• Identifying through review and improve consolidations the quantifying value adds, reducing one time and recurring costs to protect, defend, deter and remediation activities.
Residual Risk	• Reducing threat and impacts to remaining company that can occur when companies separate/ merge such as IP or exposure of critical assets, inclusive of data, network ongoing support and cyber functionality support to divested entity.

Fig 2. Key drivers and considerations for cybersecurity in Mergers & Acquisition (M&A), from transactional and IT Security perspective

Recommended Solution

As per AON survey, Cyber Attack or Data Breach is the number one risk faced by organizations globally and is predicted to remain in this position by 2026, and therefore, to mitigate cybersecurity risks in M&A transactions, a robust cybersecurity due diligence process is essential and must.

This solution should focus on a strategic approach that identifies, evaluates, and mitigates risks prior to completing the deal and serves as a whistleblower for any underlying and unknown risks. Additionally, the proposed framework should support integration planning and post-merger resilience by embedding cybersecurity considerations at every stage of the Merger & Acquisition (M&A) process.

The process can be broken down into the following steps:

Pre-Deal Cybersecurity Assessment:

- Perform a comprehensive Cybersecurity due diligence of the target Company's Information Technology (IT) infrastructure and Cybersecurity practices.
- An outside-in view supported by inside-out observations can facilitate better decisions and deal negotiations.
- Identify risk related to critical assets at enterprise level, including sensitive customer data, intellectual property, and proprietary software, to assess risk related to business continuity.
- Evaluate security governance practices, risk management frameworks, and previous breach history. A well driven and structured discussion with management and cybersecurity members on key security topics and measures can help facilitate better decisions on overall cyber governance model.

Third-Party Risk Management:

- Assess third-party vendors and service providers that may affect the Cybersecurity posture of the target company.
- Review contracts and Service Level Agreements (SLAs) to ensure adequate security and compliance clauses are in place.

Risk Evaluation Framework:

- A structured due diligence framework is essential in today's evolving threat landscape, and the steps detailed below provide the foundation for a consistent and effective assessment process.
- Develop a comprehensive risk matrix based on industry renowned standards that includes the likelihood and impact of identified cybersecurity risk and vulnerabilities.
- Conduct risk assessments to gauge security resilience across people, process and technology.

Risk Remediation and Post-Transaction Integration Plan:

- Establish short term and long-term remediation plan and align on a detailed Cybersecurity integration roadmap that focuses on bridging the gap between different cybersecurity cultures and technologies.
- Develop a post-deal cybersecurity monitoring and response plan to ensure continuous protection.
- Depending on type of transaction and entities involved, effective management of cyber risk, from initial due diligence of a target to sale preparation, can significantly impact the investment's value. Failure to address security vulnerabilities could lead to reduced valuation and increased liabilities.

Architecture Diagram and Process Methodology

By implementing the outlined approach below, organizations can systematically identify, assess, and mitigate cyber risks inherent in target entities, thereby enabling more informed decision-making during the M&A lifecycle.

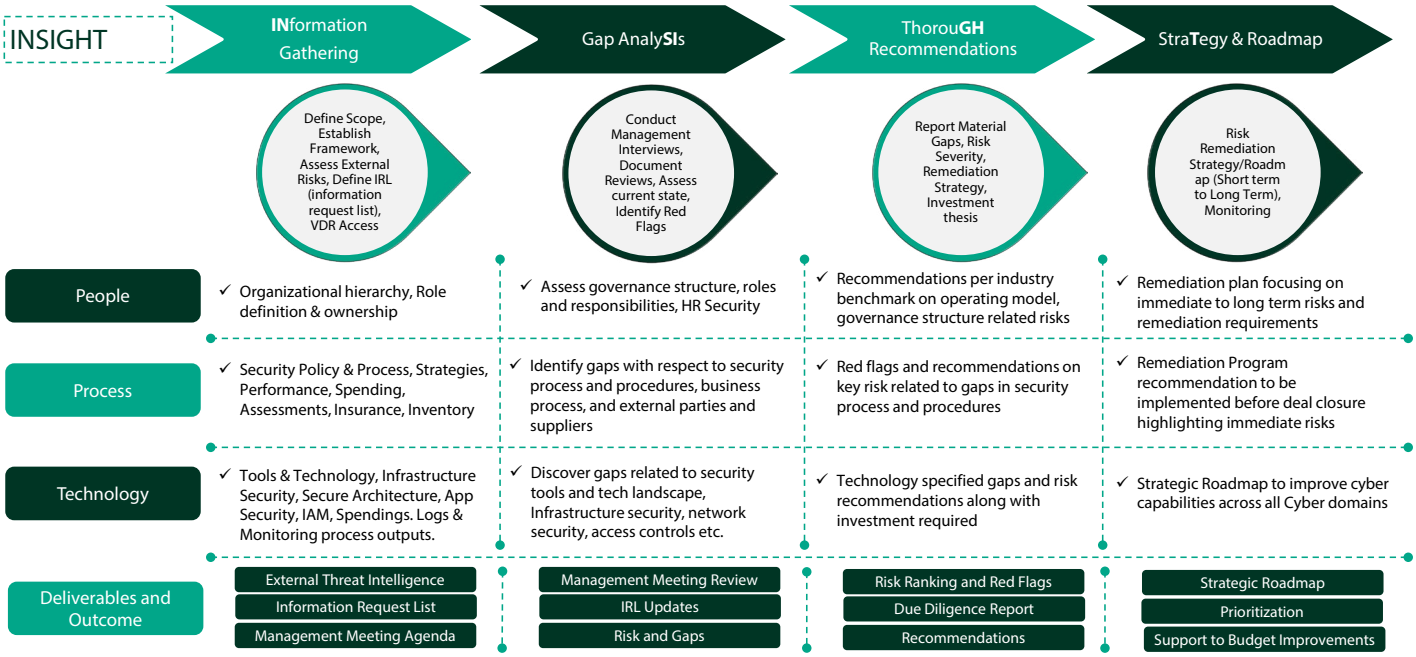


Fig 3. Key drivers and considerations for cybersecurity in Mergers & Acquisition (M&A), a fig. Infosys CyberSecurity M&A Services : Pre-Deal Service Framework

Cybersecurity Assessment:

Evaluate the target company's cybersecurity framework, and identify their strengths and weaknesses. Failure to address cyber risk could lead to major acquisition regrets. Nearly two-thirds of respondents (65%) said their companies experienced regrets in making an M&A deal due to cybersecurity concerns.

- **Tools:** Risk assessment tools, Vulnerability scanning software, Compliance checklists, Maturity Assessment, Benchmarking, Peer Comparison.
- **Outcome:** A risk profile for the company's current security posture.

Risk Identification & Documentation:

Conduct thorough reviews of IT infrastructure, cybersecurity policies, compliance records, and incident history.

- **Tools:** Risk assessment framework, data breach assessments, source code analysis, business impact analysis.
- **Outcome:** A list of high-risk areas needing attention.

Vendor & Third-Party Risk Assessment:

Evaluate third-party security practices and access control mechanisms.

- **Tools:** Third-party risk management platforms, SOC 2 reports, Third-party risk assessments
- **Outcome:** A comprehensive assessment of external and supply chain-related risks.

Cybersecurity Incident Response and Remediation Planning:

Create a strategic remediation plan to address identified risks before the deal is finalized. 73% of respondents agreed that a company with an undisclosed data breach is an immediate deal breaker in their company's M&A strategy, as per IBM's 2024 Cost of a Data Breach Report.

- **Tools:** Incident response planning, risk remediation plan, integration playbooks.
- **Outcome:** A clear roadmap for risk remediation and post-deal cybersecurity integration as per below methodology will assure risk informed decision and expedited integration.

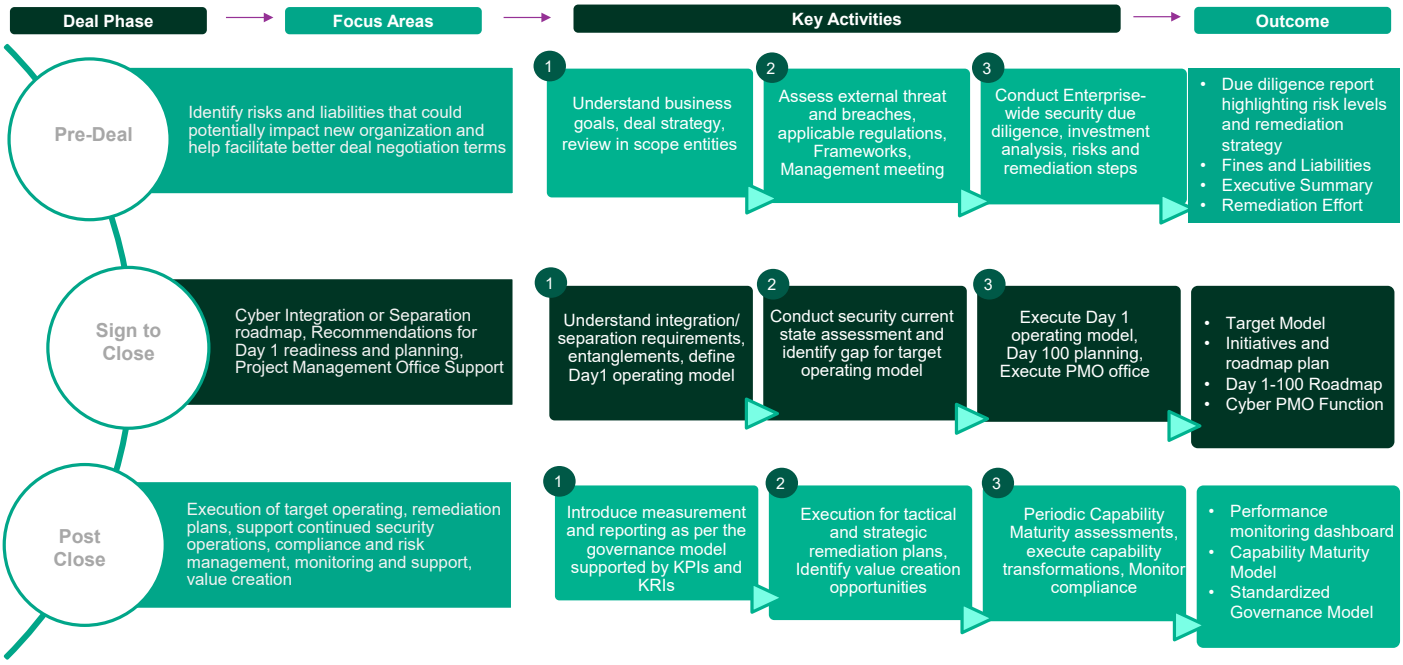


Fig 4. Infosys CyberSecurity M&A Services : Outcomes

Recommended Best Practices

Begin Early:

Start the cybersecurity due diligence process early to allow ample time for discovery, risk assessment, and mitigation.

Engage Experts:

Involve external cybersecurity experts, such as ethical hackers or specialized M&A consultants, to provide an unbiased and thorough assessment.

Leverage Automation:

Use of AI solutions and Cybersecurity tools to automate risk and threat assessments, saving time and ensuring accuracy.

Collaborate Across Teams:

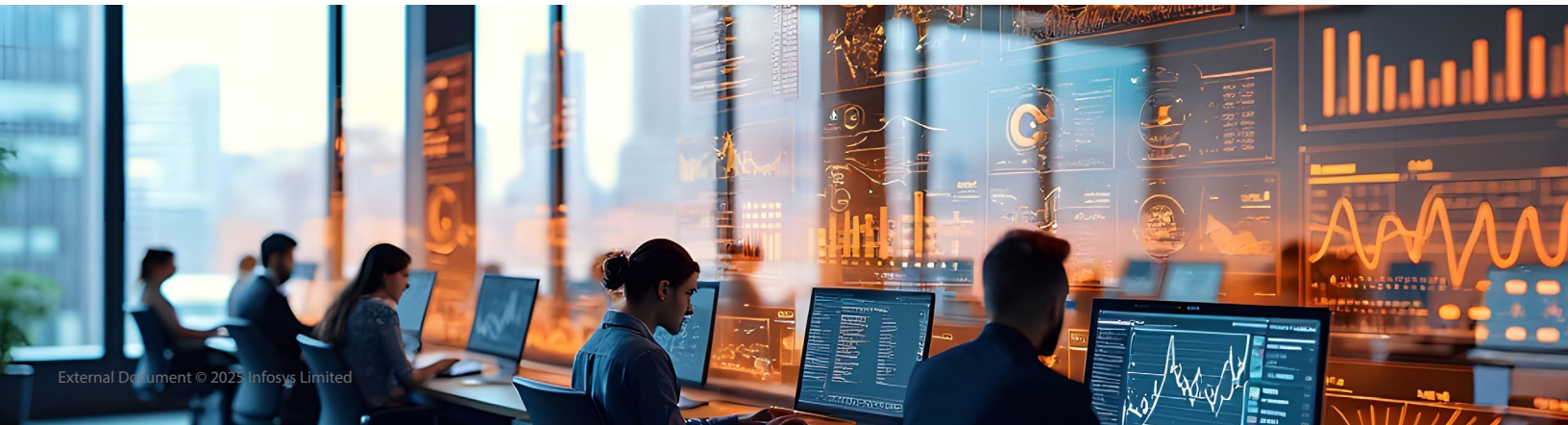
Include stakeholders from various departments—such as legal, IT, finance, and operations—to ensure that all aspects of cybersecurity risks are covered.

Develop a Post-Deal Monitoring Plan:

A solid post-deal cybersecurity strategy ensures ongoing vigilance and immediate action in case of new risks or threats.

Use Outcome-Driven Metrics for M&A Cybersecurity Due Diligence:

Cybersecurity concerns are paramount in all mergers & acquisition transactions. Outcome-driven metrics signify a game-changing approach for executive leaders to conduct timely and effective M&A cybersecurity due diligence.



Conclusion

Cybersecurity due diligence is no longer an optional consideration in the M&A process; it is essential to protect both the acquiring organization and its stakeholders from hidden cyber threats. By thoroughly evaluating the target company's cybersecurity practices, developing a clear remediation plan, and establishing a post-deal integration roadmap, businesses can mitigate risks and ensure smoother M&A transactions.

Proper planning and execution of cybersecurity due diligence will not only protect the financial value of the deal but also help preserve the long-term reputation and security of the combined entity.

References

- Forescout: forescout.com/resources/cybersecurity-in-merger-and-acquisition-report/
- IBM: Cost of a data breach 2024 | IBM
- Mergermarket & Admincontrol: Under attack: Cyber due diligence demands more of dealmakers - ION Analytics
- Aon's 2023 Global Risk Management Survey: Why It's Key to Conduct Cyber Due Diligence in Financial Services During Mergers and Acquisitions

About the Author

Nikhil Agarwal

Principal Consultant

Nikhil has over 16 years of experience in Cybersecurity and holds certifications like CISSP, CISM, and ISO 27001. He has worked with a Big 4 consulting firm, leading complex Cyber M&A projects from pre-deal due diligence to post-deal integration. His expertise includes developing cyber strategies, managing large Governance, Risk & Compliance programs, and conducting security audits across various industries and compliance standards.

Currently, he is part of a Cybersecurity Consulting & Advisory team, supporting clients with consulting, transformation, and advisory services. He also contributes to go-to-market strategies and collaborates with leadership and partners to drive business growth in cybersecurity consulting.

For more information, contact askus@infosys.com

Navigate your next