INVESTMENT AND MERGER & ACQUISITION – SECURE THE INVESTMENT

ALVAREZ & MARSAL

LEADERSHIP. ACTION. RESULTS.℠

1. Executive Summary

Create and preserve value by protecting intellectual property, mitigating critical cyber risk, complying with regulatory requirements and enhancing cyber resilience.

Mergers & Acquisitions (M&A) and investment in firms and startups have become an important part of the growth strategies of most businesses today. Most M&A integration efforts focus on elements like people, revenue, systems, finance and customer relations. Similarly, most investment focuses on market share, revenue growth and profit enhancement. However, throughout this process, cybersecurity and cyber compliance are often overlooked.

While merged entities may succeed in business integration or an investment may yield strong returns, however, any breach of confidential data, a large-scale cyberattack or non-compliance with regulatory requirements can negate these gains. Such incidents often attract negative media attention and erode shareholder value and trust. This paper highlights key issues related to intellectual property (IP) protection, data security and privacy, cybersecurity controls and compliance risks that may arise in the investee firm or during M&A IT integration and provides approaches for addressing this risk.

2. Introduction

India has been at the forefront of digital adoption and investment in technology startups have also grown multifold. With a new wave of digital transformation on the horizon, driven by the democratization of 5G, the Internet of Everything (IoT), and AI technologies, numerous startups are emerging to develop innovative products and solutions in this space. While this digital evolution offers businesses enhanced convenience and efficiency, it also brings significant cybersecurity challenges due to an expanded attack surface. In this hyper-connected digital economy, cyber threats are rapidly increasing in both volume and velocity. In the event of a cyberattack, companies may not only incur financial and operational losses but can also face long-term damage to their reputation, brand, and customer trust.

Most private equity and venture capital firms invest in technology-driven companies due to their potential for scalability, efficiency, and innovative solutions. However, after finalizing investments or acquisitions, in certain instances firms have uncovered the target company's history of data breaches, cyber threats, inadequate control, and compliance issues, leading to substantial financial losses. Cybersecurity is not a control or cost function, but a vehicle to create and preserve value.

3. Problem Statement/Challenges

Consider a hypothetical case - based on the experiences of M&A integration.

ABC Inc. in the U.S. acquired XYZ Plc. in India which had a subsidiary in the U.S. The initial integration focused on sales, technology integration, customer relations and finance. However, shortly after, several issues surfaced that required immediate attention, effort and investment, including:

- An external audit revealed weak access controls in critical systems including ERP and CRM, following the integration of the merged companies. This exposed further potential issues, such as Segregation of Duty conflicts, which required immediate attention.
- Applications, regarded as Intellectual Property due to their capabilities and use of agentic AI, were found to incorporate open-source components that violated copyright, leading to potential legal scrutiny.
- A security incident report revealed an internal breach, involving disgruntled employees who, fearing layoffs after the integration, exploited misconfigured access privileges to steal confidential documents and intellectual property.
- Constant media scrutiny of such incidents damaged the company's reputation and eroded shareholder trust.
- U.S. customer and employee data were transferred to a location specific cloud-based data center during technology integration, causing compliance and data privacy concerns.
- Post-merger, ABC Inc. had to spend a significant amount to resolve these issues, further impacting the operational efficiency of the merged entity.

In this hypothetical case study, the lack of cybersecurity controls and non-compliance might lead to costs and losses including:

1. Regulatory fines, penalties and restrictions on ability to do business like onboarding new customers.
2. Loss of productivity due to compromised systems and computing infrastructure.
3. Loss of intellectual property.
4. Violation of contractual obligations and legal risk in using open-source software.
5. Weak infrastructure, application, API and supply chain security controls can leave and organization vulnerable to cyberattacks, resulting in loss of business, trust and reputation.
6. Loss of privacy and confidential business data potentially resulting in class action lawsuits and a diminished competitive edge.

Conducting cyber due diligence prior to an investment, merger or acquisition helps organizations assess existing risks and identify issues that may warrant restructuring the agreement. This process involves evaluating the target's cybersecurity posture, policies, procedures, and controls to uncover any potential vulnerabilities.

However, it is critical to segregate the pre-deal due diligence and post deal integration. The Cyber Due Diligence (Cyber DD) or pre-deal assessments are conducted prior to finalizing a transaction and are primarily focused on evaluating the cybersecurity posture of the target entity. These assessments typically face constraints related to limited data availability and the scheduling of management meetings, which can restrict the depth and scope of the analysis. The main objective during this phase is to identify and quantify potential cybersecurity risks associated with the target company, including assessing the need for one-off investments or recurring security measures. The insights gained helps stakeholders understand the level of risk involved in the transaction and determine whether cybersecurity concerns could impact the deal's viability or valuation.

In contrast, post-deal activities—particularly during the first 100 days—are centered on executing the cybersecurity improvements identified during the initial assessment and refining the cybersecurity strategy. This phase involves implementing quick wins to address critical vulnerabilities and deepening the assessment to validate earlier findings. The goal is to develop a comprehensive cybersecurity program tailored to the specific context of the acquisition, whether it involves M&A integration, standalone operations, or a carve-out scenario. By this stage, organizations can design a detailed cybersecurity roadmap aligned with their broader strategic objectives, ensuring the target's cybersecurity posture supports long-term growth and security resilience.

4. Solution Overview

Cybersecurity due diligence is a critical component of the overall due diligence process during mergers and acquisitions (M&A) transactions. This process involves a thorough examination of the target company's cybersecurity posture, policies, and practices to identify potential risks that could affect the acquiring company post-transaction.

Below is a detailed breakdown of the steps involved in conducting cybersecurity due diligence.

4.1 Pre-Deal Cyber Due Diligence Process

We recommend a five-step cyber due diligence process:

1. Creating organization business, threat and risk profile

This step serves as the critical foundation for assessing the cybersecurity posture and identifying vulnerabilities that may affect transactions and future operations. The complexity of ecosystem, application landscape, data sensitivity, regulatory requirements and contractual obligations along with scale might change the threat, control and risk profile of the organization. Understanding the business model, operational structure, technology landscape, and strategic priorities is important for identifying the applicable threats and controls and hence its cybersecurity measures needed to protect critical assets. Modern enterprises also depend on a network of vendors, partners, and third-party service providers, which can introduce risks through indirect attack vectors. Identifying potential risks from cloud service providers, managed IT vendors, and outsourced development teams is essential for comprehensive risk assessment.

2. Conducting External Attack Surface Management (EASM)

The first step in External Attack Surface Management (EASM) is identifying all digital assets associated with the target organization, including domains, subdomains, cloud instances, applications, and third-party integrations accessible from the internet. Once these assets are mapped, the acquirer must assess them for known vulnerabilities, misconfigurations, and weaknesses that could be exploited. Additionally, acquirers should monitor underground forums, hacker marketplaces, and breach repositories to check if any corporate data or credentials have been compromised. Since external attack surfaces are continually evolving due to new technologies, changing business operations, and emerging threats, implementing continuous monitoring solutions is vital to detect and remediate newly discovered vulnerabilities or misconfigurations before they can be exploited.

3. Identifying Baseline Security Controls Based on Organization Business Context and Threat/Risk Profile

During the pre-deal and post-deal phases, identifying baseline security controls is a critical step in assessing the target company's cybersecurity posture. This process involves understanding the specific business context of the target company and evaluating its unique threat and risk profile. By considering the industry, operational structure, and existing security measures, organizations can define a set of essential security controls such as implementing Multi-Factor Authentication, hardening endpoints, asset management, effective security monitoring, etc., necessary to protect key assets and mitigate potential risks. These baseline controls ensure that the organization can defend against common cyber threats while maintaining regulatory compliance. During this step, it is important to not only assess technical aspects such as infrastructure and data security but also to ensure the existence of incident response procedures, cyber insurance coverage, and compliance frameworks to address future security incidents. Establishing these baseline controls is vital for both safeguarding the organization's assets and ensuring that the security measures align with the overall risk management strategy throughout the M&A process. The controls can be adapted from the NIST CSF standard, which assesses maturity based on the threat and control profile to reduce risk and develop a strategic plan for implementing controls, including budgeting considerations.

4. Performing Technical Security Diligence

A thorough examination of the target company's security infrastructure must be conducted to identify potential risks that could affect the value of the deal. By assessing the technical aspects of the target company's systems, networks, and applications, organization can uncover weaknesses that could lead to vulnerabilities or exploitations. This step typically involves reviewing the design and architecture of the target company's IT systems and applications, ensuring that they follow the best practices for security. It also includes evaluating vulnerabilities and configuration settings to determine if there are any misconfigurations that could expose the company to cyber threats. Additionally, validating the security of open-source software used by the target company and simulating

phishing attacks are key tactics used to identify potential risks. This technical security diligence helps to ensure that the acquiring company understands the true state of the target's cybersecurity environment, enabling them to make informed decisions and implement the necessary controls post-deal.

5. Reporting And Roadmap for Improvement/Open Exposure

This step develops a detailed report and improvement roadmap based on the findings of the previous assessments which is crucial for evaluating the current cybersecurity posture of the target company. This process helps identify any open exposures, risks, and gaps in security, providing clear recommendations for addressing vulnerabilities. The report should clearly document identified risks, weaknesses, and any compliance issues that could impact on the value or success of the deal. Additionally, the roadmap for improvement provides a strategic plan for the acquiring company to enhance the target's cybersecurity measures post-deal. The roadmap includes actionable steps, timelines, and resource requirements to address the identified vulnerabilities, ensure regulatory compliance, and strengthen overall security defenses. By providing a clear and structured approach to mitigating risks and improving security, this step helps ensure that the acquiring company can manage and reduce potential threats effectively, safeguarding its investment and ensuring long-term cybersecurity resilience.

4.2 Post Deal - Cyber Security Controls Integration

While an M&A completion marks a significant milestone, it also triggers complex and often overlooked cybersecurity challenges. As two organizations come together, so do their technology environment, with its own infrastructure, security controls, policies, vulnerabilities, and risk exposures. What's often overlooked is a deep understanding of the cybersecurity posture of each entity involved. Knowing how much time, effort, and investment it will take to integrate and secure the combined technology environment is critical to reducing post-deal risks.

The post-M&A period can introduce heightened cyber risk due to inconsistent security standards, lack of visibility across systems, conflicting access controls, and unvetted third-party relationships.

Following the M&A transaction, a strategic approach to implementing cybersecurity controls is essential. The goal is not only to unify and streamline the infrastructure but also to ensure that the merged organization is secure, compliant, and resilient. A current-state assessment of both companies' IT and security environments lays the foundation for effective integration.

Key Steps for Post-M&A Cybersecurity Implementation:

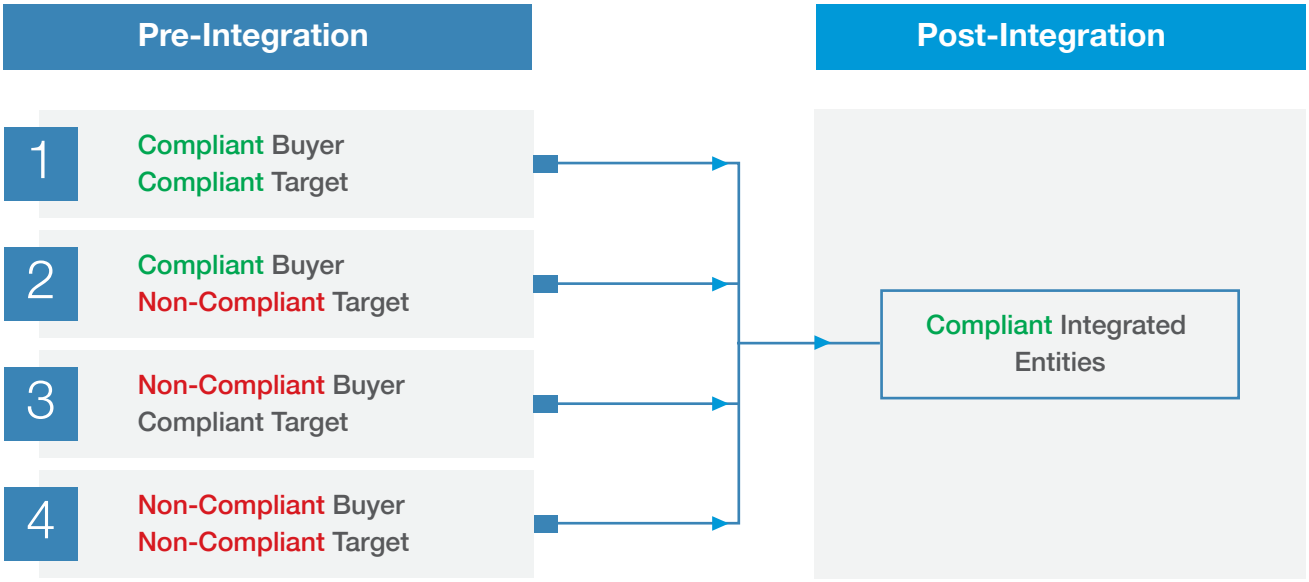
- **Identify Risk Profiles:** Evaluate the risk, threat landscape, controls, and compliance requirements of both companies, and determine the key control owners.
- **Rationalize and Align Technologies:** Examine the use of disparate technologies and identify overlaps for various technologies. This includes assessing the potential for architectural changes, such as secure segmentation, zero trust, SASE etc. to streamline operations.
- **Review and Consolidate Security Tools:** Evaluate existing security tools for overlaps and integration potential, ensuring they align with compliance readiness and feature requirements.
- **Centralize Authentication Infrastructure:** Consolidate authentication to a central store to enforce policies and security controls for authentication like MFA, Password policies, group policies and login profiles.
- **Access (Authorization) & Data Management:** Review current data storage and access management processes for customers, partners, employees, and affiliates. Implement proper controls of access governance, segregation of duties, minimum access and audit and log all access based on sensitivity.
- **Analyze Private Data:** Identify private data stored within each company's systems and track the cross-border movement of this data to ensure compliance.
- **Optimize Third-Party Security Functions:** Identify third parties involved in security functions and seek synergies to optimize operations.

Turning Assessment into Action: Strategy and Roadmap

If proper pre-deal cyber due diligence is performed and answers for the above-mentioned steps are obtained, the job is half done. The next step is to create an appropriate strategy and roadmap to address these issues for the combined entity. This strategy should prioritize key areas such as governance and compliance, access management and data protection, protection of intellectual property, and data privacy.

1. Governance And Compliance

In any M&A deal, aligning cybersecurity and compliance post-integration is crucial to ensuring long-term stability and regulatory adherence. While the primary focus often remains on financial and operational aspects, overlooking cybersecurity compliance can expose the newly formed entity to significant risks. The following figure highlights common compliance scenarios during acquisitions and emphasizes the importance of proactive planning to achieve a secure and compliant integration.



Since cybersecurity, risk, and compliance are not typically considered primary drivers during integration, companies may receive a limited-time waiver to meet compliance requirements. As a result, management often deprioritizes risk and compliance tasks, only to realize the complexity and urgency of these issues later in the process, with much less time available for resolution.

Technology too, plays an essential role in implementing effective controls and should be thoroughly integrated into compliance initiatives. This integration must be approached in a formalized and structured manner to ensure that compliance requirements are met efficiently and without delay.

2. Access Management

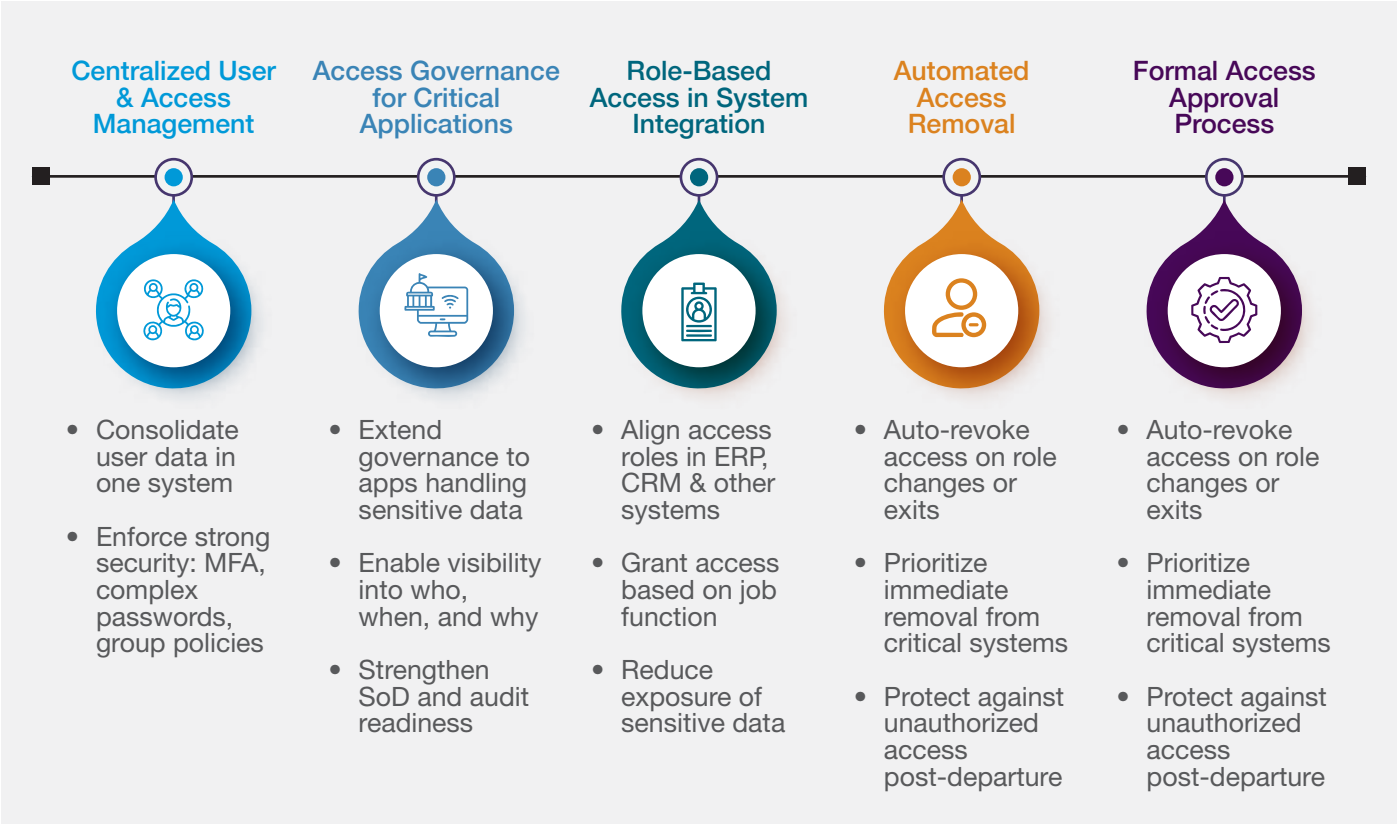
When two companies merge, they inevitably combine their data as well. This presents a unique challenge: even if both companies had previously implemented robust data protection and access management strategies, the merger opens new avenues for unintended access to that data. The integration process can inadvertently expose sensitive information to individuals or systems that should not have access to it.

To address this risk, it is crucial to identify the systems and data that need protection early in the merger process. The first step is to classify the combined data into categories based on its sensitivity and access needs. This allows organizations to apply appropriate levels of security to different types of data. By carefully mapping out data stores, identifying data flows, and understanding how and where data moves across systems, companies can establish clear guidelines for authorized data usage, storage, sharing, and access.

An essential part of this process is implementing technical controls to ensure that data is only accessible to those with the necessary permissions. This involves creating visibility into data access patterns and monitoring for any unauthorized activity. Furthermore, it is important to take a fresh look at the roles and responsibilities of users within the organization. Existing roles may need to be redefined, or new roles may need to be created to ensure that data access is granted only to individuals who genuinely require it. This process, known as role-rationalization, helps minimize unnecessary access and potential security risks.

Controlled Access is a key

A strong access-management system not only safeguards company assets but also plays a pivotal role in ensuring smooth and secure integration between organizations. Here are some key strategies for achieving controlled access during the integration process.



3. Data Protection, Information Rights Management and Protection of Intellectual Property

During the complex process of mergers and divestitures, safeguarding sensitive documents and intellectual property is a top priority for any organization. Information Rights Management (IRM) is key to ensuring that only a select group of individuals has access to sensitive data, particularly documents related to the transaction itself. This is especially crucial in industries such as pharmaceuticals and manufacturing, where intellectual property and proprietary information must be carefully protected.

The first step in safeguarding sensitive information during mergers or divestitures is identifying and classifying the data. Companies must clearly understand which documents and processes are vital to the transaction, enabling them to apply the necessary security measures to restrict access and prevent unauthorized sharing. Another equally important aspect is defining the "trusted community"—the select group of individuals who require access to sensitive data. Limiting access to only those directly involved in the merger ensures that confidential information is protected from unauthorized exposure.

Given the dynamic nature of data, companies must also plan for a sustained phase of data protection. This involves continuously monitoring and updating security measures to adapt to changing business needs and evolving risks. Some important ongoing activities include:

- **Data Leakage Incident Management:** Establishing procedures for identifying and responding to data leaks or breaches as they occur.
- **Audit and Fine-Tuning of Data Protection Solutions:** Regularly reviewing and refining security solutions such as Data Loss Prevention (DLP), IRM, and Digital Asset Management (DAM) to ensure they remain effective in preventing unauthorized access or misuse.
- **Awareness and Policy Updates:** Continuously educating employees about data protection policies and finetune DLP and IRM rules to reflect the organization's changing business needs.

4. Data Privacy

During mergers and acquisitions, companies should very seriously think about data privacy and their compliance and security.

In the realm of information security and privacy, personally identifiable information (PII) refers to any data that can be used to uniquely identify, contact, or locate an individual. The protection of PII has become increasingly critical due to the rise of outsourcing, data proliferation, BYOD and software as service usage. With the new DPDA act, fines and penalties are significant along with breach of trust impacting customer retention in case of privacy breaches.

Prior to inking the deal, the acquirer should be aware of the potential security problems of the target company to be acquired. Considering the risks associated with data security breaches, privacy related risks should be included in the due-diligence checklist. An apparent advantage of studying these issues prior to integration is better insights into the potential risks and hence helps in determining various aspects of the deal these may affect like planning for cost, efforts, controls required, timeline, liabilities, etc.

Several factors related to privacy must be considered to determine the level of focus, effort, and applicable regulatory requirements during integration. Among these, two stand out as particularly important:

Industry Type: Different industries like financial services, healthcare, IT, etc. handle different types of private data and are governed by different compliances and regulations. For example, healthcare organizations must comply with HIPAA, while financial institutions may be governed by regulations like GLBA. Understanding the specific compliance obligations of each sector is essential for effective integration.

Geographic Footprint: Privacy laws vary significantly across regions. For instance, European regulations like the GDPR are more stringent compared to those in the United States. In today's landscape of increasing cross-border mergers and acquisitions, it is crucial to evaluate the impact of data movement across jurisdictions. When the buyer and target operate in different countries, integration planning must account for the complexities of international data transfers. Failure to address these issues can lead to regulatory violations, reputational damage, stock price impacts, and a loss of shareholder confidence.

Once the key pillars of cybersecurity — governance and compliance, access management, data protection and protection of intellectual property and data privacy – are addressed, the cyber integration aligns seamlessly with the broader technology integration efforts, enabling a smooth and secure transition for the combined ecosystem.

5. Benefits of Due Diligence and Cyber Integration during M&A

Integrating cybersecurity considerations into the M&A process is no longer optional—it's a strategic necessity. Beyond protecting against threats, cybersecurity due diligence ensures that the acquiring and target companies align on risk management, compliance, and operational resilience.

A well-executed cyber integration not only safeguards digital assets but also lays the foundation for long-term business continuity and stakeholder trust. The following are some of the key benefits of embedding cybersecurity into the M&A lifecycle.

Visibility into Cyber Risk Posture
Gain a clear understanding of current threats and required cybersecurity investments to ensure secure operations.

Protection of Intellectual Property
Safeguard critical assets, proprietary data, and innovations from breaches and misuse.

Regulatory Compliance
Ensure alignment with industry standards and regulatory frameworks across regions.

Third-Party Risk Management
Identify and govern risks associated witih vendors, partners, and service providers.

Customer Data Privacy
Implement strong controls to protect customer information and maintain compliance with privacy laws.

Trust in the Digital Ecosystem
Strengthen stakeholder confidence and reputation by demonstrating cyber ressilience.

6. Conclusion

In today's landscape of heightened public scrutiny and increasing regulatory demands, companies cannot afford lapses in compliance, unauthorized access, critical cyber incidents, or the loss of sensitive data and intellectual property. While traditional due diligence efforts may touch upon technology, they often overlook the depth required in cybersecurity assessments.

To avoid unpleasant surprises, ensure risk transparency, and minimize the likelihood of non-compliance, organizations must treat cybersecurity due diligence as a core component of the M&A process—not an afterthought.

So, how do you know that your M&A strategy effectively addresses compliance, risk and security?

- Involve data privacy, security and compliance professionals early in integration planning phase
- Evaluate and address the full spectrum of components of risk, security and control elements
- Continuously monitor and adapt throughout the process

By embedding cybersecurity into your M&A framework, you not only protect the value of the deal but also build a resilient and secure foundation for the newly integrated entity.

CONTACTS

CHANDRAPRAKASH SURYAWANSHI (CP)
Managing Director and India Global
Cyber Risk Services Practice Leader
csuryawanshi@alvarezandmarsal.com

ABOUT ALVAREZ & MARSAL

Founded in 1983, Alvarez & Marsal is a leading global professional services firm. Renowned for its leadership, action and results, Alvarez & Marsal provides advisory, business performance improvement and turnaround management services, delivering practical solutions to address clients' unique challenges. With a world-wide network of experienced operators, world-class consultants, former regulators and industry authorities, Alvarez & Marsal helps corporates, boards, private equity firms, law firms and government agencies drive transformation, mitigate risk and unlock value at every stage of growth.

To learn more, visit: **AlvarezandMarsal.com**

Follow A&M on:

ALVAREZ & MARSAL
LEADERSHIP. ACTION. RESULTS.℠