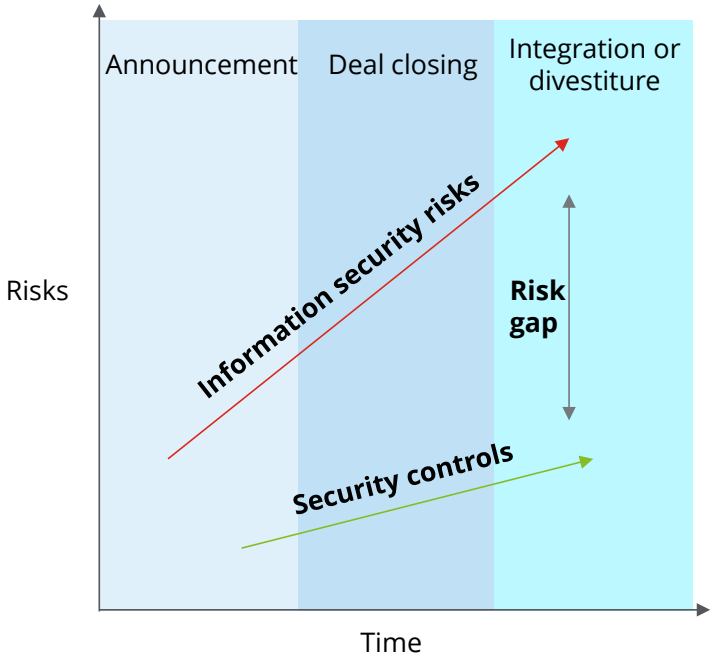
Deloitte.

Don’t drop the ball

Identify and reduce cyber risks during M&A

As if M&A deal teams didn’t have enough balls to juggle during a transaction’s lifecycle, today’s complex and porous digital marketplace is tossing in one more – increased cyber risk. Every stage of M&A – strategy, screening, due diligence, transaction execution, and integration – is subject to heightened risk for cyber threats and attacks which, if not discovered and defused, could harm both the acquirer and target…and even scuttle the deal.

Figure 1: Cyber risks in the M&A lifecycle



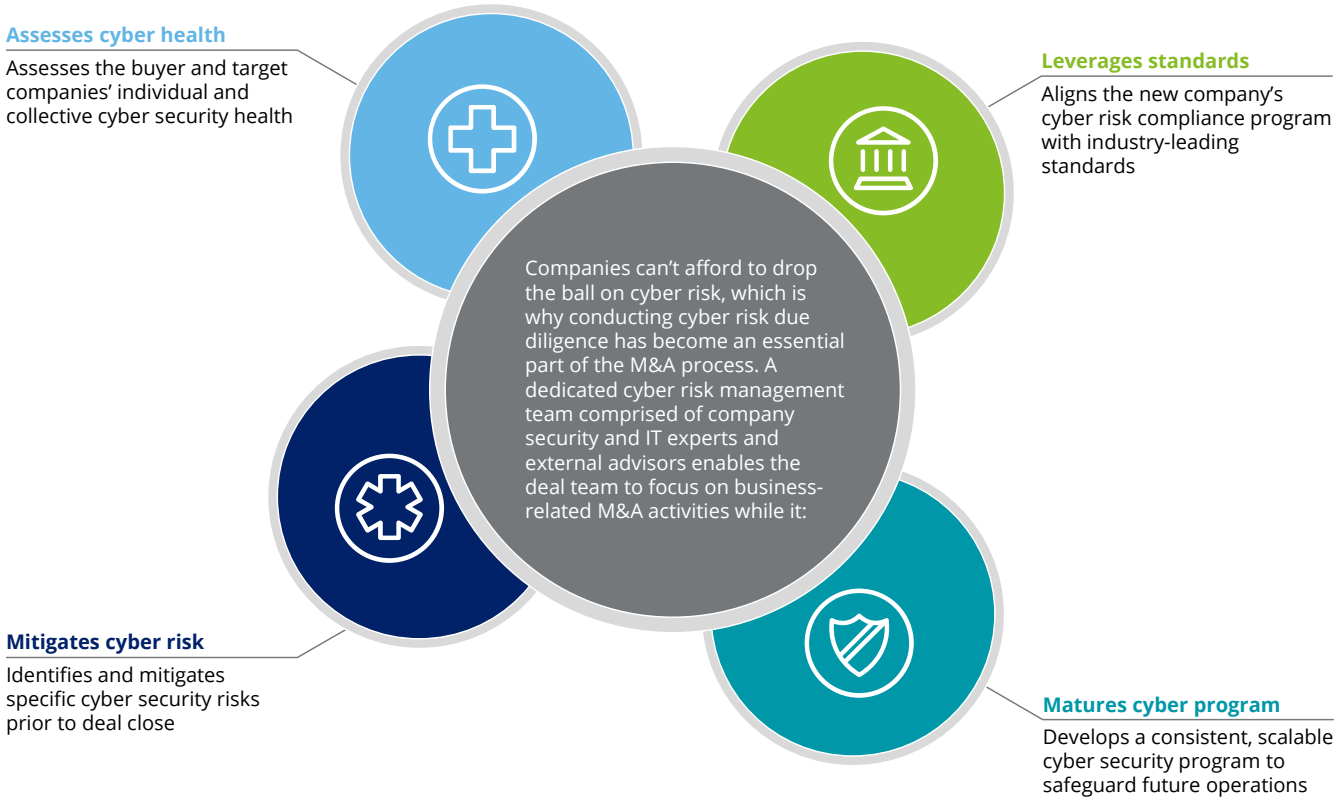
Source: Deloitte & Touche LLP, 2016

Cyber risks vary from one M&A lifecycle stage to the next, and may be generated both internally and externally. Common risks include:

- Targeting from a cyber threat actor leading to damaged reputation with Wall Street and potential stock devaluation;
- Failure to understand and mitigate deep cyber shortcomings (including legal and regulatory risks) in the target company;
- Reaching a deal price that does not accurately reflect the cyber health and robustness of the seller’s networks and systems that will form the basis for a new division of the acquiring company;
- Unknowingly exposing the acquirer’s enterprise network to threat of cyber attack when integrating potentially antiquated and unpatched systems and IT assets of the target company

Engaging the cyber risk management team prior to initiating the M&A process can provide strategic value at each stage in the deal lifecycle.

Figure 2: Cyber risk due diligence



M&A strategy

Prior to launching an M&A transaction, the cyber risk management team should develop a corporate risk assessment strategy and playbook to guide cyber risk-related due diligence consistently for each potential M&A target, with defined requirements and expectations for cyber risk controls. This playbook can help reduce the level of ad hoc and deal-specific project planning and increase the speed and reliability of the company's overall cyber due diligence process. Once this pre-planning is complete, acquisition targets can be sought out and compared to the existing strategy.

Playbooks are typically comprised of two major components: the cyber risk due diligence approach and the associated tools and templates. The due diligence approach identifies organization-specific drivers to align the cyber risk due diligence with broader corporate strategy. To enable the most effective results, the approach should lay out high-level timelines and milestones and identify a core team of subject matter experts for each deal. The timelines and milestones should be flexible enough to recognize variable deal complexity (e.g., a complete merger of overlapping business functions between two highly-regulated companies is likely be more complex and multidimensional than a straightforward purchase of IP assets in a non-regulated industry).

The tools and templates section of the playbook should identify and include documentation and reference materials for executing the approach, including a cyber assessment framework, checklists to enable and track information requests, sample questions, and project management templates.

Screening and due diligence

Once a potential acquisition target has been identified, the next phases typically involve target screening and in-depth due diligence. Target screening identifies potential acquisition candidates, or potential acquirers for a company wishing to sell itself entirely or in part. Due diligence provides the opportunity for the acquirer to conduct discovery on the acquisition target, including analyzing or financial stability and health, review of cyber risk and infrastructure, or interaction with acquisition target leadership to gauge interest in an M&A transaction.

A number of tools and methodologies are available to support target screening. Activities often include conducting high-level research to create a target company's threat profile, identifying instances of historical cyber risks (e.g., published examples of breaches), and providing industry-level insights. The resulting report should be helpful in driving and/or scoping follow-on due diligence efforts.

Once a target has been selected and passed through the initial screening, due diligence is fully initiated, and the cyber risk management team should coordinate the due diligence activities related to cyber risk. At a foundational level, cyber risk assessment activities typically employ a custom-designed framework that leverages industry leading practices, globally recognized standards, and unique requirements that reflect the acquiring company's deal drivers. The framework should facilitate a holistic review of a target's cyber risk, including an in-depth analysis of its IT governance, operations, information security, business continuity, physical security, and overall risk posture.

The assessment generally consists of three core methods that may be used in parallel: offline document and system review (typically handled via a virtual data room), onsite workshops, and cyber risk profiling. One or more of these methods may not be appropriate or necessary in all contexts, however, as every deal has its own nuances and complexities. The offline document and system review includes analyzing documentation, resources, and artifacts (e.g., system architecture documents, information assets) to develop an understanding of the acquisition target's environment and identify preliminary findings and remediation opportunities. In addition to the document review, the cyber risk management team may determine it appropriate to conduct vulnerability assessments and penetration testing on the target's IT systems. While this testing typically focuses on perimeter weaknesses, the scope and scale can be readily adjusted to fit the situation.

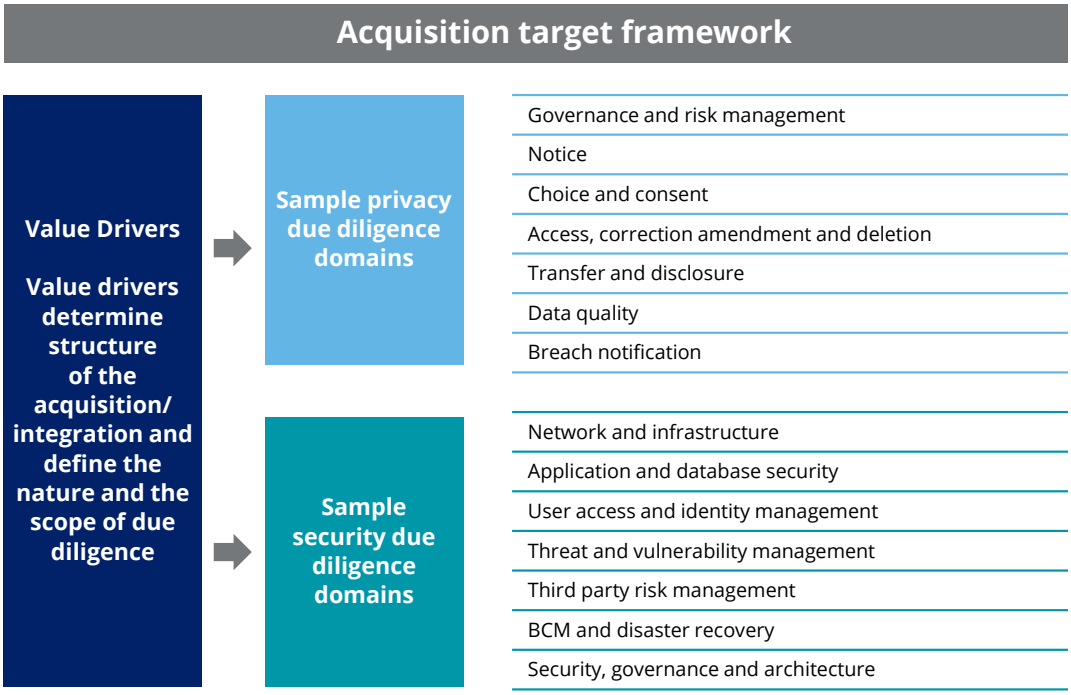
The second core method is the onsite workshops, which typically take place at the acquisition target's corporate facilities, including data centers, where appropriate. The cyber risk management team meets directly with leadership, management, and subject matter experts to identify and discuss risks, findings, and remediation opportunities. In some cases, the acquiring company will send additional representatives. When this occurs, the risk management team will typically operate as a central project management office (PMO) to coordinate schedules, align content to reduce overlap, and lead workshop activities.

The final assessment method – cyber risk profiling – includes two avenues: cyber reconnaissance and compromise diagnostics. With the acquisition of the target company's assets, the acquiring company also receives certain aspects of the target's threat profile. Cyber reconnaissance and threat profiling can assist in identifying techniques, tactics, and procedures that threat actors employ against companies experiencing large-scale, organizational change. Cyber reconnaissance provides a company undergoing a transformation a point-in-time assessment of its exposure to cyber threats by assessing the company's assets across relevant intelligence sources. Reconnaissance typically includes conducting threat assessments that leverage ethical hacking and penetration testing techniques, and that use open, closed, and proprietary sources and underground criminal forums. The resulting cyber threat profile provides insight into the criticalities that threat actors may target and how.

Based on knowledge gleaned from the reconnaissance and threat profile, the acquiring company may wish to perform a gap analysis and cyber diagnostic to determine if the target is already compromised. Advanced attackers specifically evade the cyber risk tools and technologies companies traditionally leverage. With this in mind, a diagnostic can review the target's environment to identify active or dormant threats present on its computer systems and networks. The review assesses endpoints and network traffic transiting between the target organization's networks and the Internet. It deploys agent-based endpoint technology to all desktops, laptops and servers to search and review for potential Indicators of Compromise to identify anomalies, malware, vulnerabilities, or other conditions that would pose a threat to the organization.

Once the risk management team has completed assessment activities, it may compile a cyber risk mitigation plan that includes a detailed review of each risk with prioritized tactical steps for remediation. The plan also identifies suggested owners for remediation activities, forecasts costs, and may even recommend a preliminary end-state IT infrastructure to support cyber risk-related integration activities.

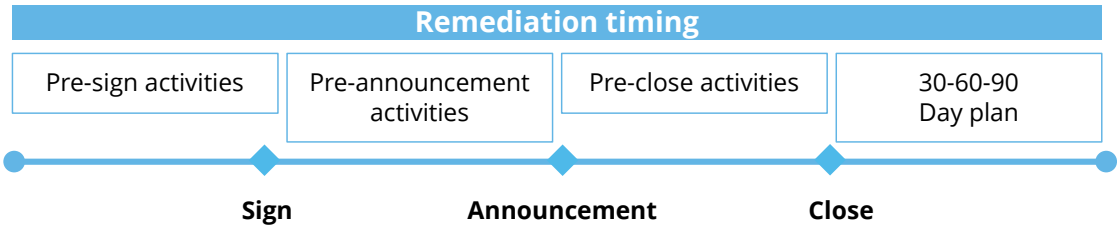
Figure 3: Acquisition target framework



In some cases, this remediation plan may require mitigation activities prior to Day 1, but usually after the deal is signed. These mitigation activities are tailored to address the highest severity risks, especially those that may lead to issues. When identifying these activities, the risk management team should account for additional activity and interest from threat actors that can occur once the acquisition is publicly announced.

Finally, the remediation plan may also be used as leverage in the deal-making process itself. The costs associated with remediation of significant cyber risks may be used as a lever to reduce the overall acquisition costs. For example, if the acquisition target requires the development and implementation of a network demilitarized zone (DMZ) to be stable on Day 1, some or all of the costs of that project may be subtracted from the overall valuation of that company. This process requires careful coordination between company leadership and cyber risk management subject matter experts in order to convey the appropriate messaging to the acquisition target, syndicates and attorneys involved.

Figure 4: Remediation timing



Transaction execution

The cyber risk management team's involvement in an M&A transaction does not end after target screening and due diligence. The acquirer's prime objective in this phase is to facilitate an uneventful, issue-free Day 1. During this phase, the deal team may ask for assistance with cyber risk remediation activities and advise on integration plans for network architecture, and support technology (e.g., e-mail servers, human resources systems). Tasks may include reviewing the asset inventory developed during the due diligence phase to outline recommendations for logical and physical access provisioning, and identifying, developing, and implementing controls and processes to support Day 1 activities. Other relevant activities include reviewing critical system redundancies, planning for back-up and storage requirements, creating incident response procedures, and ramping-up cyber threat monitoring and vulnerability management capabilities.

Integration

An issue-free integration starts long before an M&A deal closes. Both companies participate in the integration process, where the two entities are merged according to the terms of the deal and the overall M&A strategy of the acquirer. The cyber risk assessment results may prompt the newly combined company's IT and cyber security staff to address a number of findings, improvement opportunities, and integration activities. To drive this effort, remediation and integration activities are typically summarized in a prioritized "30-60-90 plan," with target milestones laid out at 30-days post-close, 60-days post-close, 90-days post-close, and beyond.

Within the first 30-days post-close, the IT and security teams should address critical or high risk remediation activities, especially in cases where onsite remediation cannot occur prior to Day 1. Activities usually include developing strong perimeter security, addressing substantial gaps in business continuity, and closing critical or high-risk vulnerabilities. Additionally, the end-state cyber risk infrastructure should be developed and revised, with foundational technologies and devices implemented as needed.

Once the 30-day milestones have been addressed, the 60-day and 90-day activities should include re-testing and re-assessing solutions implemented as part of the earlier plan, and performing additional remediation for medium- and low-risk findings and vulnerabilities. Issues vary greatly from company to company and typically are prioritized based on factors unique to that environment. Finally, the cyber risk management team should play a key role in safeguarding the new company's IT systems, applications, and online presence. Common responsibilities include:

Identity and access management

M&A typically spawns reorganization and restructuring, which require heightened identity and access supervision. Ongoing identity and access management (IAM) services facilitate administration throughout the user lifecycle, from on-boarding to off-boarding enterprise users (e.g., employees, contractors, vendors, customers). Along with identify management comes the need to administer and monitor access privileges and roles. Access management is critical to organizations that may be shifting large amounts of enterprise resources. Services include access control and configuration support, and maintaining user profiles, entitlements, and application access rules. Familiarity with the leading IAM technology vendors, such as Oracle, IBM, CA, SailPoint, EMC/RSA, CyberArk, Lieberman, is also key to effectively implementing an IAM solution.

Enterprise application integrity

A company merger can present a challenge to managing and protecting critical assets due, in part, to evolving threats that accompany the integration of business environments. A portion of this challenge is related to enterprise resource planning (ERP). When expanding and extending beyond traditional corporate IT borders, it is critical to address ERP system security, privacy, control, and compliance requirements. Enterprise application integrity (EAI) services help promote data security across the application ecosystem and within related business processes.

Managed Threat and SIEM

Organizations must remain ever-vigilant to cyber security threats. This means having overarching visibility and pre-emptive threat insights to detect known and unknown adversarial activity. To be able to accomplish this, the cyber risk team should work with internal and external resources to develop managed threat services (MTS) solutions that enhance in-house capabilities and increase the value of Security Information & Event Management (SIEM).

Threat intelligence analytics

A company's ability to manage cyber threats and have a trusted SIEM operation depends heavily upon its ability to operationalize an organization's cyber threat intelligence program. During and after M&A activity, mitigating business risk should be a priority that requires timely, insightful, and predictive analysis tailored to the company's changing environment. Effective, actionable threat intelligence analytics provides the context and prioritization necessary to support recommendations for risk mitigation.

Don't drop the (cyber) ball

Conducting cyber risk due diligence has become an essential part of the M&A process. A dedicated cyber risk management team can provide strategic value at each stage in the deal lifecycle by assessing, identifying, and reducing potential cyber security risks prior to and after deal close.

Contacts:

David Mapgaonkar
Principal
Advisory Cyber Risk Services
Deloitte & Touche LLP
dmapgaonkar@deloitte.com

Arun Perinkolam
Principal
Advisory Cyber Risk Services
Deloitte & Touche LLP
aperinkolam@deloitte.com

M&A
Institute

About the Deloitte M&A Institute
The Deloitte M&A Institute is a community of clients and practitioners focused on increasing the value derived from M&A activities, powered by Deloitte's M&A Services capabilities. The Institute serves as a platform to build connections, showcase thought leadership, and accelerate experience and learning for those involved.

Deloitte.

About Deloitte
Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. Please see www.deloitte.com/about for a detailed description of DTTL and its member firms. Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries. Certain services may not be available to attest clients under the rules and regulations of public accounting.