NISOS
Webinar Brief

The Evolution of Cyber Diligence in Mergers and Acquisitions

Executive Summary

In this webinar, cybersecurity, private equity, venture, and consulting leaders from Workday, Astra Capital, Momentum Cyber, Chertoff Group, and Nisos discuss the evolution and importance of cyber due diligence in mergers and acquisitions.

Cyber due diligence is not only a process of protecting an asset, it is also a process that must look at business context and objectives. The "buy side" typically has two main objectives aligned to the stages of the deal:

1. **Pre-Close:** Identify and inform business stakeholders of cyber, non-traditional, and key man risks related to the acquisition based on off-network, "outside the firewall" collection of data.
2. **Post-Close:** Develop an understanding of "known risks" based on off-network findings as well as on-network findings and disclosures from the acquired organization during the integration process.

Transparency in the Cyber Due Diligence Process

The biggest change in the last five years is that the buy-side board of directors are asking questions concerning risks inherent in technology platforms and network infrastructure. They are concerned with cyber risks affecting the confidentiality, integrity, and availability of data, systems, and networks.

In addition, they are concerned about their ability to insure against inherited cyber risk. While the industry recognizes the importance of cyber diligence, risk that was previously mitigated through insurance coverage may no longer be discharged that way.

Insurance carriers are now removing coverage from policies and indicating that if a business has more than $100 million in enterprise value, they will no longer insure for cyber risk.

No standard exists for cyber due diligence and the practice is evolving. Cyber risks continue to exist in silos (architecture, controls, roles and responsibilities, IT integration, etc). Given the short timeframes associated with acquisition due diligence, it's difficult to establish and quantify metrics and frameworks.

Any business being acquired is scrutinized for future earnings potential. Part of this diligence process includes checks and balances to ensure the proper insurance is in place to mitigate risk factors from potential loss cyber insurance when possible. It's important to have subject matter experts with dedicated and flexible runbooks ready to act when an acquisition target is identified. The runbooks should include:

1. Reviewing and understanding the means by which sensitive customer data or technology platforms are or could be compromised.
    - Scans and consultative risk assessments to review potential vulnerabilities and cyber maturity hygiene (asset management, patching, security controls).
    - Open source and dark web analysis of chatter related to breaches, leaks of proprietary information, negative sentiment, and key personnel.
    - Technical review of external attack surface management for compromise or derogatory information against the target of acquisition and key suppliers (malicious traffic flows for malware, operational integration concerns).
2. Using cyber tools as a means of diligence to complete background checks for the business and key stakeholders.
3. Diligence and review of businesses in the cybersecurity community confirm representations of business and ensure differentiation.

Business Context is Critical

The technical aspects of a deal, when evaluated by technical teams performing the cyber diligence, are commonly complex when it comes to the question of vulnerabilities. In M&A, the answers aren't binary and, unfortunately, business is not black and white.

Part of cyber diligence is identifying the amount of risk that can be tolerated and the types of questions that can be left unanswered, while continuing to move the deal forward. Diligence efforts must highlight issues to address after the deal is finalized and the integration of organizations has begun.

Expectations have evolved. Five years ago, boards, bankers, and insurance executives understood cybersecurity was important and "would not tolerate any cyber risk". However, they didn't understand the overall impacts of cyber due diligence findings, and as a result good deals were getting killed before closure.

Cyber due diligence is not aimed at killing deals. **The gold standard for cyber due diligence is determining "reasonable security controls" and an operating plan to implement when the deal closes. Understanding diligence findings can drive the process and the plan.** In some cases, security controls may be part of a future earn out on the part of the target of acquisition. This is based on factors that may include:

1. Type of business being bought, including the sensitive data or technology being acquired.
2. Maturity of the business being acquired relative to security controls and compliance processes in place at the time of the deal.

Example: a ransomware event takes place against a technology company (the value of the business is less than $100 million) during the acquisition due diligence phase. In this case, the buyer is going to take a 51% controlling stake in the business. The resulting investigation determines architectural design flaws in the code that enabled the breach to occur. Consequently, a complete redesign of the code base is required. These findings may result in lenders being uncomfortable and thus kill the deal.

Alternatively, if the ransomware event occurred due to a pair of credentials found on the dark web and the lack of two factor authentication, (a more manageable issue), it will be less costly to implement a fix, and will likely be more acceptable to lenders.

About Nisos

Nisos is the Managed Intelligence Company™. Our services enable security, intelligence, and trust & safety teams to leverage a world-class intelligence capability tailored to their needs. We fuse robust data collection with a deep understanding of the adversarial mindset delivering smarter defense and more effective response against advanced cyber attacks, disinformation and abuse of digital platforms. For more information visit: **www.nisos.com**