COHN REZNICK
ACCOUNTING • TAX • ADVISORY

CYBERSECURITY *INSIGHTS*

Forward Thinking Thought Leadership

November 2017

Considering a Merger or Acquisition? Build Cyber Diligence into Your Target Assessment

In today's digital economy, executives rely heavily on information systems and data stored within those systems to operate their business and make sound corporate decisions. Organizations are dependent on IT assets to create, use, communicate, and store critical and sensitive information, including generating financial statements. Such increased dependence on IT assets and information in electronic form increases an organization's susceptibility to cybersecurity threats—leaving a business vulnerable to major harm to both its operations and stakeholders in the event of a security breach.

For companies seeking a merger or acquisition, the primary goal of due diligence has traditionally been to investigate the target of an M&A transaction to gain a deeper understanding of the target's business operations, its financial condition, assets, liabilities, and overall health of the business. However, the heightened reliance on networked infrastructure, systems, and use of emerging technologies adds a necessary layer to the due diligence process—cyber diligence. Also referred to as cybersecurity due diligence, cyber diligence is rapidly becoming an essential component of the overall review process.

Cyber Diligence Assessment Areas and Key Benefit

Doing a cyber diligence assessment on a target company's IT environment can have an impact on how an acquirer values and structures a deal. It is important for acquiring organizations to understand the target company's vulnerabilities and the potential scope of the damage that may occur, or may have already occurred, in the event of a breach. In addition, it is critical to evaluate the adequacy and effectiveness of cyber defenses the target business has implemented to protect and defend itself from the ever-changing cyber threat landscape.

While cyber diligence may not always provide complete assurance of the target company's ability to protect and defend against cybersecurity threats, it can provide reasonable understanding and assurance of the target company's current capabilities and its IT environment. A cyber diligence assessment can bring to light the actual condition of the target's IT assets by revealing the cyber vulnerabilities of those assets; whether the target has been adequately safeguarding and monitoring the control of those assets; and any records of security incidents that may have resulted in a breach and compromises of those assets and the data within the assets.

Devising a Cyber Diligence Strategy

Cyber diligence cannot be based on a one-size-fits-all approach. As with any diligence effort, the scope and coverage of any cyber diligence effort depends on the transaction timeline, as well as the target company's industry, regulatory environment, value of IT assets, and overall cybersecurity risk profile.

While cyber diligence should consider and include evaluation of a target's IT environment, such as its IT strategy, governance, and processes, a cyber diligence strategy should specifically focus on the following key areas to understand the cybersecurity posture of the target company:

- **Cybersecurity strategy, governance, and culture.** Understand and evaluate whether the target company has established an adequate cybersecurity strategy and has good governance around ensuring that cybersecurity processes and controls are working adequately. Strong cyber processes and controls should defend and protect against cybersecurity threats from both external malicious attackers and from internal users falling prey to clicking links and providing sensitive information via email, allowing intruders through the network.

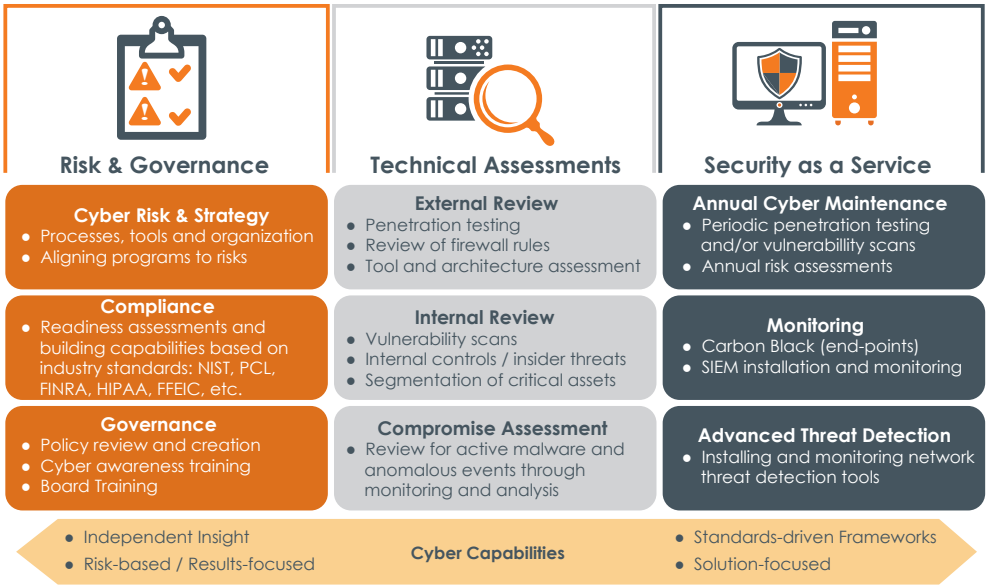
  Equally important is to evaluate whether adequate security awareness training is provided to employees frequently by target company management. Is the culture one of identifying, detecting, and notifying IT management or responsible parties if employees see something malicious?

- **Alignment with industry standards and best practices.** Does the target company's cybersecurity strategy and program meet the relevant industry standards for cybersecurity practices and procedures? How mature is the cybersecurity program? Special consideration should be given to the maturity of the company's vendor management programs; cybersecurity insurance policies and any indemnification clauses; current and past cybersecurity incidents and how they were handled; and communication with internal and external parties, specifically customers, regulators, law enforcements, and third parties regarding security incidents and breaches.

- **Regulatory requirements.** Does the target company have to comply with any regulatory requirements geared toward cybersecurity, security incident reporting, and privacy? Has the company demonstrated compliance? When was the compliance examination last conducted on the target company's network or IT infrastructure?
- **IT infrastructure and security:** "Seeing is believing" and "Trust, but verify" are principles that strongly apply in the case of cyber diligence. The acquiring company's diligence team cannot simply rely on a target company's assurances without conducting verification checks or independently validating the security posture of the target company's IT environment. Oftentimes, organizations don't prioritize security, and organizations with security weaknesses or vulnerabilities seldom recognize the problem.

  An acquiring company should verify if the target company has recently engaged a third party to undergo a vulnerability assessment and penetration testing of their network. If the target company has not done so, then the acquiring company should retain a firm to independently test the target company's IT infrastructure and network. The test should also gather intelligence related to whether the target company was breached and if any customer information, or the target company's intellectual property, was compromised and is available for sale on the dark web. Alternatively, the acquiring company should require the target company to engage an independent third party for vulnerability scanning and penetration testing. The comprehensive report showing the results of the testing should be available to the acquiring company for review.

A thorough cyber diligence program should align with the components shown below:



Key Takeaways

The heightened reliance on IT assets and their equal vulnerability to a cybersecurity breach calls for a necessary new component to the due diligence process when preparing for an M&A transaction. Uncovering a target company's cyber vulnerabilities, the scope of damage that could occur—or has already occurred—as well as evaluating existing cyber defenses implemented by the target company could meaningfully impact how an acquirer values and structures a deal. A successful cyber diligence strategy should be scaled based on the nature, size, and complexity of the acquiring and target companies involved in the transaction.

Contact

For more information on building a cyber diligence strategy—whether your need is to develop a high-level cybersecurity risk assessment, to conduct independent vulnerability scanning and penetration testing, or to assess the entire IT environment for technical threats and exposures at any layer in the technology stack—contact:

Bhavesh Vadhani, Principal and CohnReznick Advisory's Cybersecurity Practice Leader, at Bhavesh.vadhani@cohnreznick.com or 703-847-4418

About CohnReznick's Cybersecurity Services

CohnReznick provides cybersecurity solutions that are dynamic, scalable, and tailored for growth companies. CohnReznick's security professionals average more than 15 years in the field and hold key certifications. Our professionals have deep experience assisting organizations in implementing and complying with information and cybersecurity requirements using NIST 800-53, ISO 27001, COBIT, CIS, and other leading standards and frameworks.

About CohnReznick

CohnReznick LLP is one of the top accounting, tax, and advisory firms in the United States, combining the deep resources of a national firm with the hands-on, agile approach that today's dynamic business environment demands. With diverse industry expertise, the Firm provides companies with the insight and experience to help them break through and seize growth opportunities. The Firm, with origins dating back to 1919, is headquartered in New York, NY with 2,700 employees in offices nationwide. CohnReznick is a member of Nexia International, a global network of independent accountancy, tax, and business advisors. For more information, visit www.cohnreznick.com