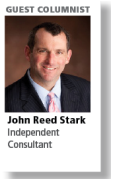
COMPLIANCE WEEK
THE LEADING INFORMATION SERVICE ON CORPORATE GOVERNANCE, RISK, AND COMPLIANCE

Cyber-security due diligence: a new imperative

John Reed Stark | June 7, 2016



Show me a company with weak cyber-security and I will show you a company with lackluster corporate governance, anemic C-suite leadership, and head-in-the-sand operations. Hence, the rise of a new, specialized and complex business demand in the corporate world: cyber-security due diligence.

Cyber-security due diligence is rapidly becoming a critical factor of the decision-making calculus for a corporation contemplating a merger, acquisition, asset purchase, or other business combination; an organization taking on a new vendor, partner, or other alliance; or a private equity firm purchasing a new portfolio company.

In every industry, cyber-security weaknesses represent a significant risk to the operations, reputation, and the bottom line of all companies, whatever their size and wherever their location. The mantra underlying cyber-security due diligence concerns is simple: No matter what the terms, when adding, partnering, or working with another enterprise, a company is taking on that company's data troubles and attendant data risks.

Corporate vendor management

Given that cyber-attackers will often traverse across a company's network and gain entry into the networks of its vendors or vice versa, third- party vendors have become one of the more prevalent attack vectors, so for corporate vendor management, cyber-security due diligence has become similarly essential.

Cyber-criminals have launched some of the most damaging attacks of the past few years through third parties. In fact, numerous studies have shown that third parties represent 40 percent to 80 percent of the risks associated with data breaches. Three recent examples illustrate the issue: (1) CVS confirmed a data breach of its photo service, which remains offline after hackers allegedly breached PNI Digital—a third-party vendor that manages CVS's photo website; (2) Cal State University was breached through an outsourced firm that provided online courses for violence prevention; and (3) the Army National Guard reports that the data of 850,000 current members have been exposed due to an improper data transfer to a third party non DoD-accredited data center for a data analysis.

The use of third-party vendors has also become a cyber-security concern for regulators, including the SEC, FINRA, and New York State Department of Banking Services.

Thus, for some companies, including financial firms and banking institutions, third-party cyber-risk management is not only a security function, but also a compliance obligation.

Corporate business combinations

For corporate mergers and acquisitions and other changes in control, vigorous cyber-security due diligence not only better informs deal terms and deal value but can also signal early deal-breakers, saving buyers from unforeseen financial costs, regulatory liabilities, technological integration headaches, or even bankruptcy.

Aside from offering additional opportunities to more closely assess the risk of business combinations, cyber-security due diligence analysis can impact valuation and contracting issues as well. Without a fully developed understanding of a company's cyber-security profile, a company cannot:

- Appreciate the value of another company, whether acquisition target, partner, or vendor;
- Identify and execute opportunities for strengthening cyber-security; and
- Draft data-related provisions in the transaction or vendor's agreements, so that where possible, parties can implement post-transaction cyber-security solutions. The virtual evolution of due diligence

Despite the fact that cyber-attacks remain a steady concern across industries, far too many due diligence teams have still failed to recognize information security as a key data point for decision making. Instead, due diligence teams continue to focus on the more traditional information technology (IT) categories of inquiry, such as a company's technological systems and any associated integration issues. This needs to change.

Just as in the financial accounting realm, stale due diligence models should be modified and enhanced to address the ever-increasing enterprise threat of cyber-attacks. Cyber risks are real and costly, and the most forward-thinking companies assess the cyber-health and safety of an enterprise before committing to a significant investment or

Related articles

Avoiding Vanguard's cyber-security stumble (http://www.complianceweek.com/blogs/john-reed-stark/avoiding-vanguard%E2%80%99s-cyber-security-stumble)

The SEC's Newly Proclaimed Search Warrant Authority (http://www.complianceweek.com/blogs/john-reed-stark/the-sec%E2%80%99s-newly-proclaimed-search-warrant-authority)

What Makes a Good 'Pen Tester' (http://www.complianceweek.com/blogs/john-reed-stark/what-makes-a-good-%E2%80%98pen-tester%E2%80%99)

Transforming the Cyber-Security Paradigm (http://www.complianceweek.com/blogs/john-reed-stark/transforming-the-cyber-security-paradigm)

> Take heed from the adage, "If you want success, you should start with your health," because in today's world of cyber-attacks and state-sponsored virtual terrorism, "If corporations want success, they should start with their cyber-security."

relationship. Likewise, a company or vendor can strengthen its attractiveness as a partner or a takeover target by conducting "self" cyber-security due diligence to demonstrate the fitness of its enterprise.

Traditionally, due diligence efforts are geared toward identifying the markets, geographies, technologies, synergies and strategic angles of a business relationship. For instance, at the outset of an M&A deal or a new partnership, due diligence teams scrub financial statements, recasting and recalculating them in every conceivable way to determine the viability, sustainability, and profitability of a deal. Due diligence teams should apply the same energy, breadth, and intensity to evaluating a company's cyber-security.

Cyber-security due diligence and the cloud

Cloud storage has many potential advantages for companies, including cost savings, scalability, increased mobility, and easier collaboration. However, when storing critical and/or confidential information in the cloud, that information is essentially stored off-site, possibly in another country, so companies must make sure to use cloud providers that can provide meaningful assurances regarding overall data security.

Along the same lines, cloud-based file sharing services, such as Dropbox, Google Drive, Box, and others, are another way confidential information leaks out of a company. Unbeknownst to many companies, cloud services like Dropbox are often used through personal accounts (despite many large companies prohibiting, as a matter of policy, the use of such services for these purposes). Some companies also block access to such services from the company's desktop computers with effective security controls, while other companies are less sophisticated or simply resist the notion of becoming the automated "data nanny" for their employees.

Given the increased adoption of cloud-based services by enterprises of every kind, cyber-attacks on cloud environments have almost reached the same level as attacks on traditional IT. Whether as a phase at the front end of an acquisition-related corporate transaction or as an aspect of a company's vendor management, cyber-security due diligence teams should probe a company's cloud-related practices, especially an assessment of any enterprise-grade security systems and analytics; a determination of the attack vectors; and data security measures.

Just a few of the many questions to consider include: whether cloud data is encrypted (in transition and in motion); who holds encryption keys; whether cloud data is subject to search and seizure (domestically and internationally); the specifics of the cloud firm's security systems, incident response capabilities, and risk resilience; what cloud logging exists and is maintained; whether cloud data can be subject to a litigation hold or other restrictions; whether cloud data can be transferred to a data discovery tool for review; whether the cloud firm undergoes annual penetration testing and risk and security assessments; what regulatory and privacy requirements apply to cloud data; and whether the cloud firm and the company have indemnification agreements and cyber-insurance.

Due diligence teams also should confirm that a company has a comprehensive means to prevent sensitive data from being uploaded for inappropriate sharing and the requisite visibility and access to detect anomalies, conduct further investigation, and take quick and decisive remedial action.

Cyber-security due diligence and business development

The result of rigorous cyber-security due diligence can reveal more than a company's abilities to deter and manage a cyber-attack. A robust and resilient cyber-security profile also indicates strong potential for business development.

For instance, in addition to documenting a company's planned response to a cyber-attack, an incident response plan can also serve as a powerful marketing and business development tool. More and more, customers, partners, and other collaborators and fiduciaries are asking to review companies' incident response plans and factoring their value and efficacy into their hiring and procurement calculus. Maintaining a top-notch incident response plan not only indicates a company's superior preparation efforts against cyber-attacks but also indicates the leadership of a smart, organized, informed, and focused C-suite.

Along these lines, CISOs have quickly become business development leaders, as their workload has evolved into far more than internally maintaining and strengthening a company's cyber-security infrastructure. CISOs are now a key corporate asset for managing and assuaging external cyber-security concerns, such as those stemming from a company's clients, customers, partners, and other fiduciaries. Nowadays third parties, whether buyers or collaborators, need more than just reassurance about cyber-security risk; they require a robust, meaningful, and objective analysis directly from the CISO.

Cyber-security due diligence and corporate well-being

Data security concerns are not the only reason it should be standard practice for due diligence deal teams to embed cyber-security subject matter experts with the more traditional business, legal, and technical workflow of due diligence exercises. There is an even more important purpose: to gauge overall corporate health and hygiene.

When a cyber-security due diligence team finds problems and weaknesses, it is more than just a red flag indicating cyber-attack risks; it also evidences a distracted and detached C-suite and perhaps even an inattentive board of directors. And the reverse rings equally true. Like the pre-med student who aces organic chemistry, any company earning high cyber-security grades is a rarity; probably grades high in every other subject; probably has the intelligence, fortitude, and grit to overcome and thrive amid any future challenge; and probably makes for a strong future and dynamic partner.

Take heed from the adage, "If you want success, you should start with your health," because in today's world of cyber-attacks and state-sponsored virtual terrorism, "If corporations want success, they should start with their cyber-security."