July 8, 2015

LAW BUSINESS TECHNOLOGY
BUSINESS TECHNOLOGY LAW
TECHNOLOGY LAW BUSINESS
THE RECORDER
daily at www.therecorder.com
An ALM Publication

Get a Handle on Third-Party Cybersecurity Risks

Jason Straight, UnitedLex

Jason Straight

Corporate counsel have a new responsibility: cyber risk management. It's no longer just an IT problem. The inexorable convergence of legal and information security is turning the centuries-old legal culture on its head, as corporate legal departments and law firms scramble to meet the security demands—and related liabilities—of the digital age. Reference the recent report from Citigroup's cyberintelligence center, which notes that many law firms—which typically host sensitive information on their networks about corporate deals and business strategies—have weak security standards, compared to their corporate clients.

Corporate counsel, as the owners and managers of law firm relationships, must now consider cybersecurity risks in their selection process and must work with firms to mitigate security concerns and issues. However, while law firm risks loom large for corporate counsel, corporate legal departments must also be aware of vulnerabilities emerging from across the entire spectrum of contractors, partners and vendors with which their organization does business, whether that means an HVAC company (the vector in the Target breach), a point-of-sale equipment vendor (the culprit in several attacks on retailers), an IT vendor or a prestigious international law firm.

No one should be shocked to learn that third-party vendor security has become a top priority for enterprises of all kinds in 2015. And in the wake of the Anthem breach—Anthem being one of the nation's largest third-party vendors—many companies are finally paying attention to the third-party threat. A 2015 Forrester survey of IT security and risk management decision-makers at enterprises in the U.S., the U.K., France and Germany indicates that organizations are more concerned that third parties pose a risk of critical data loss (63 percent of respondents) and cyberattacks (62 percent) than they are about their vendor's ability to deliver quality and timely service as contracted (55 percent). An impressive 79 percent consider "ensuring business partners/third parties comply with our security requirements" a critical or high-priority IT security priority.

Such sentiments would seem to indicate we are entering a new stage of awareness, at least in IT departments. Whether legal departments are following suit is still an open question, but legal and regulatory events in recent years are most certainly difficult signs for legal departments to ignore. Yet today, many in-house counsel only get involved in third-party risk in two circumstances: (1) reviewing contract terms and conditions; and (2) responding to a data breach incident.

With the Target breach came an unprecedented expansion in security breach litigation. Not only did shareholders file suits, but banks sued to recover losses incurred as they struggled to clean up the mess. The recent judgment against Target has ensured that this new expanded breach litigation landscape will become the norm.

The Federal Trade Commission has been acting to enforce cybersecurity standards for many years, and although Wyndham Worldwide and LabMD are challenging the agency's authority, those appear to be losing battles. Regulatory enforcement at both the federal and state levels is expanding, with cases like the Anthem breach acting as a catalyst. For example, the Anthem incident prompted New York's Department of Financial Services to announce broad new efforts to tighten the rules surround-

ing insurance companies and their partners, including imposition of "regular, targeted assessments of preparedness," "enhanced regulations" and, notably, "stronger measures related to the representations and warranties insurance companies receive from third-party vendors." New state and federal regulations will only add to the complexities and responsibilities associated with third-party risk management.

Yet in spite of increasing federal scrutiny and the very real possibility that a data breach could result in crippling litigation, soaring costs, loss of customer good will and devastating publicity, many corporations still fail to properly vet their third-party vendors. All too often, an organization's third-party risk mitigation stops at standard indemnifying language and a simple security checklist, failing to secure access for its security team and security providers to test and verify the vendor's security. Even those companies that have formal vendor risk management programs fail to take into consideration all the potential legal and regulatory risks presented by a given third-party relationship.

So what should legal be doing to get a handle on third-party risk in the enterprise?

It's time for corporate legal departments to stand up and assume a proactive role. Today, cybersecurity is as much a legal problem as it is an IT problem, and successful mitigation requires a unified and collaborative approach. Information security practitioners may understand the IT ramifications of a security breach, but they are much less likely to understand the legal, regulatory and business implications as comprehensively as the legal team.

Begin by identifying and classifying areas of risk. Legal is uniquely positioned to provide insight and guidance to IT particularly in the identification and classification of risk. Work with information security professionals—and preferably with stakeholders in compliance, HR and management as well—to understand the value of your data assets, then assess and classify the potential threats, including the exposure of data handled by third parties. Going through this exercise will provide a more complete view of your risk landscape and allow you to take a strategic approach to securing your data.

Classifying vendors according to enterprise risk allows your information security team to prioritize its most rigorous oversight activities on higher-risk vendors. Such vendors might include IT hosting or co-location data center providers, cloud or software-as-a-service providers, financial service providers such as payroll processors or processors of medical and insurance claims, for example. Be careful, however, not to make easy assumptions about vendors and risk. While many companies might initially think of an HVAC vendor as low risk, that was decidedly not the case for Target.

Collaborate with your CISO and security team to drive policy, facilitate enforcement and draft strong contracts. Once data assets, risks and security requirements have been classified and mapped, it's time to leverage the knowledge-sharing that went in to that process to draft strong contracts ensuring that all third-party vendors are thoroughly vetted, that your information security team has visibility into and access to third-party infrastructure and employee practices, and that actionable incident response and disaster recovery plans are in place.

Legal stakeholders will be able to collaborate more effectively with the cybersecurity team to drive policy and draft those strong vendor contracts if they are familiar with these security "basics." Legal departments that take the trouble to educate themselves now about the risks third-party vendors pose, and take appropriate steps to assess and manage those risks, are much less likely to find themselves scrambling in the future to deal with the fallout of a major security incident.

Jason Straight is the Senior Vice President and Chief Privacy Officer at UnitedLex. He has more than a decade of experience assisting clients in managing information security risks, data breach incidents, data privacy obligations and complex electronic discovery challenges. He is a frequent speaker and author on topics relating to data privacy, cybersecurity, data breach response and computer forensics.