paloalto NETWORKS®

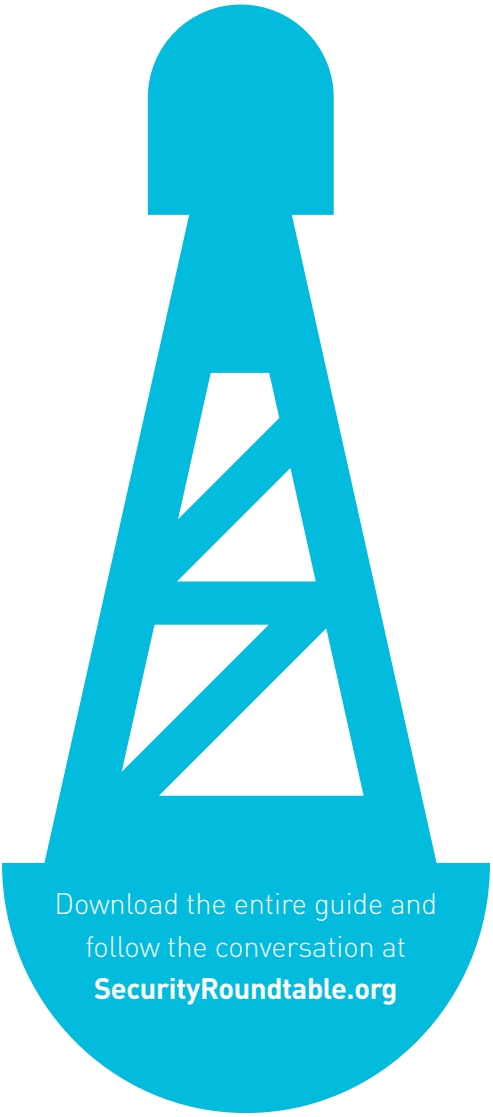
NYSE

NAVIGATING THE DIGITAL AGE

THE DEFINITIVE CYBERSECURITY GUIDE FOR DIRECTORS AND OFFICERS

Georgia Tech Institute for Information Security & Privacy

INTERNET SECURITY ALLIANCE


Download the entire guide and
follow the conversation at
SecurityRoundtable.org

21

Cybersecurity due diligence in M&A transactions: Tips for conducting a robust and meaningful process

Latham & Watkins LLP – Jennifer Archie, Partner

To begin with a tautology, when you buy a company, you buy their data—and the attendant risks to that data. Cybersecurity risks are not limited to consumer-facing businesses, whose recent losses of cardholder or patient data grab news headlines. Indeed, few businesses today have assets and liabilities that are not in some sense data driven. For most business combinations—whether M&A, joint venture, or leveraged buyout—cybersecurity should be a risk category in its own right. Buyers should review not just historic breaches but also cybersecurity risk management. Even though these risks are hard to quantify, the analysis will inform deal terms, deal value, and post-deal indemnity claims.

First step: Get an early read on cyber readiness at the engagement stage

Buyers should begin all cybersecurity risk assessments early in the engagement process, with the goal of clearly articulating as early as possible the target company's most important information assets, systems, and business processes. Every target business should be able to readily identify which information technology (IT) systems and data sets are most valuable to the business and explain at a high level how the company protects and exploits them. Even at the earliest stages, the seller should be prepared to identify and discuss the following at a high level:

- What types of information or computer systems and operations are most important to your business? What sensitive types of data do you handle or hold relating to natural persons (which data elements in particular)?
- Where is sensitive information stored?
- How is it protected in transit, at rest, and in motion?
- What are the most concerning threats to information, networks, or systems?

- Have there been prior incidents?
- What is the cybersecurity budget?
- What are your recovery plans if critical information or systems become unavailable?

If the front line deal-facing personnel respond, "I don't know, I'd have to ask," this is a telling and interesting sign that the target company's security management program is likely not well integrated into the senior leadership ranks. Sellers thus should be prepared in early discussions to showcase a sophisticated understanding of data security risks and how those risks may materially affect the company's operations, reputation, and legal risks (or not). A buyer's key diligence objective should be to probe and test whether the target company has implemented a mature risk management organization to evaluate the accuracy of management assurances about lack of historical breaches, payment card industry (PCI) compliance, protections against competitor or insider theft, and business continuity. Too often in hindsight, a target's statements made in diligence turn out to have been good faith impressions, or even merely aspirational or reflective of paper policy, but not operational reality.

Tailor diligence to what types of information are handled and how important is information security to the bottom line

Beyond these general questions, the buyer should directly probe whether the target management has a sophisticated understanding of potential cyber-related liabilities and the regulatory environment. Unlike environmental or traditional fire or natural disaster scenarios, cyberattack-related liabilities are multi-faceted and unique. In some industries—such as energy, transportation, financial institutions, health care, defense contracting, education, and telecommunications—government oversight can be active and intrusive, and the target's subject matter expertise will likely reside within the legal, compliance, and/or IT functions. In other industries, however, exposure to costly government investigations from the Federal Trade Commission (FTC) or other agencies may be poorly understood. Federal investigations tarnish brands, especially if enforcement results. Investigations are expensive and distracting, and may lead to a sweeping 10- or 20-year permanent injunction dictating how future information security will be managed and monitored. Compliance with such a decree is expensive and limits a company's independence and flexibility in significant ways. After a breach, management is often surprised to learn how persistent and aggressive the FTC or state attorneys general can be, even if the company sees itself as a victim of harm, not a perpetrator of consumer injury. If the target's legal or business representatives are not knowledgeable about the regulatory and enforcement environments, buyers should not place much weight on a seller's lulling statements or assurances that there have been no incidents or that risk of a cyber event is low.

Check for integrated cyber risk awareness and mitigation and a comprehensive security management program

Another sign of a mature security program is a management team with cross-functional awareness on these points at the CEO and board levels, as reflected in board minutes or other documentation. A security program will not be effective if it is a silo inside the IT or information security functions. All substantial stakeholder departments should be involved in cybersecurity risk management, including business unit leaders, legal, internal audit and compliance, finance, human resources, IT, and risk management.

Diligence questionnaires should ask the target company to generally summarize the administrative, technical, and physical information security controls currently in place to safeguard the most critical business data sets. Such controls include technical measures (such as boundary and malware defense, data encryption, intrusion detection systems, anomalous event monitoring, and access controls), administrative measures, and

physical security. The company should have a current documented crisis management/incident response plan in place, including pre-staging of legal and forensic experts and a public relations strategy, all approved by senior management. A seller should specifically inquire about and assess what financial resources are applied to data security, in the context of the target's overall approach to risk containment and specific to its industry. Also, sellers should ask the following to gather detailed information about how the company has organized the management of cybersecurity and risk:

- Is there a single designated person with overall responsibility? To whom does he or she report? (Risk Officer? CTO? CIO? CEO?)
- Describe board oversight. Have directors and senior managers participated in data security training/been involved in the development of data security protocols?
- Does the company have legal counsel regularly advising on data security compliance? Is counsel internal or external, and if external, who?
- How does the company educate and train employees and vendors about company policies, information security risks, and necessary measures to mitigate risk?
- How can employees or members of the public (such as independent security researchers) report potential vulnerabilities/breaches, including irregular activity or transactions?
- What is the plan to recover should critical or other necessary systems become unavailable? What are the recovery point and recovery time objectives? How have these and other elements of the plan been correlated to business needs?

If the company has in the last year or two completed an internal or external audit or assessment to determine compliance with company security policies and/or external security standards, this should be requested, or at a minimum the target company should report whether all recommendations have been adopted, budgeted and scheduled, or already implemented.

For companies whose vendors hold company-sensitive data or access systems, the company should have implemented—prior to engaging in a business relationship—a formal vendor management program that specifically assesses risk and identifies potential security or data privacy concerns and appropriate remediation next steps. After a decision to engage, the company should mitigate data security risks through written agreements and supervision. These third parties should have data security insurance coverage and/or the agreements should require such a party to defend and indemnify the target company for legal liability arising from any release or disclosure of the information resulting from the negligence of the vendor or other third party. Third-party agreements involving data exchange or access also should articulate breach notification procedures, cooperation levels, information sharing, and expressly assign incident control and reporting responsibilities.

Cloud-based or other software-as-a-solution (SAAS) solutions as well as mobile devices present their own cybersecurity risks and should not be overlooked in diligence. Does the company permit employees to use cloud-based file-sharing services? Does it rely on SAAS solutions for critical or other business needs such as contact relationship management or HR? Email? How are the security and compliance risks presented being managed? Companies that issue or support mobile devices should have policies and procedures in place designed to protect sensitive information in those environments.

Use subject matter experts to assess cyber readiness and liabilities

Given the importance of the above questions, the buyer should pay careful attention to who asks these questions on behalf of the buyer or underwriters, in what settings, and with what time allowances. Put simply, deal teams ideally should embed subject matter experts on the business side,

the technical side, and even the legal side early on—to do the following:

- Pose questions orally
- Follow up with document requests
- Assess the documentation
- Conduct on-site testing and analysis where appropriate
- Assess and advise on the maturity and suitability of the program to the underlying data risks
- Review and advise on deal terms or costs to remediate gaps in compliance or risk management.

Very importantly, the deal team also must be nimble and focused upon the specific industry, because cybersecurity risks are highly variable across industry sectors; threats, liabilities, and government expectations for adequate security are evolving constantly. For example, if hackers acquire and then resell large databases of cardholder data to identity thieves—as happened to Target and Home Depot—the types of expenses and liabilities a buyer could expect are well documented in SEC filings. Expenditures include the following:

- Costs to investigate, contain, and remediate damaged networks and payment systems and to upgrade security
- Liability to banks, card associations, or payment processors for fines, penalties, or fraudulent charges
- Card reissuance expenses
- Expense of outside legal, technical, and communications advisors.

For retail sector, diligence surrounding PCI compliance should seek more than a "yes" or "no" response

Buyers of companies who accept, process, store, or handle cardholder payment data streams of course will want to pay particular attention to compliance with current PCI standards. At Home Depot, for example, an attacker used a vendor's username and password to gain access to Home Depot's network. The attacker then acquired elevated rights that allowed it to navigate portions of the company's systems and to deploy unique, custom-built malware on self-checkout systems to access the payment card information of up to 56 million customers who shopped at U.S. and Canadian stores between April 2014 and September 2014. In fiscal 2014, alone, Home Depot recorded $63 million in pretax expenses related to the data breach, partially offset by $30 million of expected insurance proceeds for costs believed to be reimbursable and probable of recovery under insurance coverage, resulting in pretax net expenses of $33 million.

What this sort of financial and reputational exposure means for M&A diligence within the retail sector is that buyers should devote expert and highly substantive attention to how cardholder data are collected, stored, handled, and secured. Payment processing services are material to all retail businesses, and all payment processing agreements have PCI compliance as a material term. So just as the SEC always wants to know about where that relationship stands in its review of risk factors, buyers too want to pay special attention in this area. If PCI compliance is lacking, the seller should at least be able to disclose a specific remediation timeline and a budgeted plan that is hopefully supervised and accepted by the payment processor.

PCI compliance handled correctly is costly and involves constant adaptation and optimization to new threats and new standards. It is not an annual "check-a-box" process. Within the data security space—as was true for Home Depot, Target, and many others—good business practice assumes that a compromised merchant will have a recent, valid, self-certification or even third-party certification of PCI compliance. However, a buyer should not rely simply on the inclusion of such a report or certificate in a virtual data room. Many a breached retailer has held a current PCI certification. Accordingly, the buyer should always test the security of cardholder data independently, at a process

level if necessary. The same security consultants who arrive post-breach to assess root cause and damage can examine card-related data security very meaningfully in the M&A setting, even with only a few days of on-site interviews and document collection. If PCI compliance concerns arise in diligence, deal terms can be arranged that mandate and appropriate funding for third-party independent assessments and implementation of recommendations. Moreover, many retailers now are migrating to new payment systems, and this is a unique technology risk because of the likelihood of delay, interruptions, and budgetary over-runs.

Understand and assess awareness and mitigation of risks of trade secret theft, nation-state espionage, and denial of service attacks

Beyond payment card security risks, theft of trade secrets by competitors and insiders, state-sponsored espionage that is exploited for economic advantage, and cyberattacks that disable or cripple corporate networks are less publicized but can be equally damaging to a target business. For example, the high-profile, studio-wide cyberattack at Sony Pictures in November 2014 at the hands of a group calling itself #GOP, aka the Guardians of Peace, starkly illustrates the potential to cripple a business. The attack, which the FBI attributed to North Korea, resulted in the theft of terabytes of company internal email and documents, release of unreleased movies to file-sharing networks, deletion of documents from Sony computers, threatening messages to the company and individual employees, theft and apparent exploitation of sensitive human resources data, and a near complete and prolonged disruption of the company's ability to transact business and communicate electronically over its networks and systems. In an interview with CBS News, Sony's outside cyber investigator, Kevin Mandia, disclosed that 3,000 computers and 800 servers were wiped, and 6,000 employees were "given a taste of living offline"—no email and no way to process employee benefits or time cards (Source: http://www.cbsnews.com/news/north-korean-cyberattack-on-sony-60-minutes/). To add insult to injury, much of the exfiltrated material is now readily available (and free text searchable) on WikiLeaks.

The potential for outright theft of intellectual property by competitors should not be overlooked. In *DuPont v. Kolon* (*United States v. Kolon Industries, Inc. et al.*), for example, the manufacturer of Heracron, a competitor product to DuPont's Kevlar, misappropriated DuPont's confidential information by hiring former DuPont employees as consultants and pressuring them to reveal Kevlar-related trade secrets. DuPont sued the competitor, Kolon, in 2009, and in 2012 the Department of Justice brought criminal trade secret misappropriation charges against Kolon and five of its executives pursuant to 18 U.S.C. § 1832. In light of the parallel charges, Kolon settled, paying $360 million in damages—$85 million in fines and $275 million in restitution. (Source: Department of Justice Office of Public Affairs, http://www.justice.gov/opa/pr/top-executives-kolon-industries-indicted-stealing-dupont-s-kevlar-trade-secrets). To assess these sorts of risks, acquirers should ask:

- Are there former employees who had access to critical intellectual property or other company confidential information who have recently left for competitors?
- What agreements are in place to protect the proprietary information they have?

U.S.-based businesses, academic institutions, cleared defense contractors, and government agencies increasingly are targeted for economic espionage and theft of trade secrets by foreign competitors with state sponsorship and backing. In the last fiscal year alone, economic espionage and theft of trade secrets cost the American economy more than $19 billion. According to the FBI, between 2009 and 2013, the number of arrests related to economic espionage and theft of trade secrets—which the FBI's

Economic Espionage Unit oversees—at least doubled, indictments more than tripled, and convictions increased sixfold. These numbers grossly understate the frequency of such attacks or losses. Last year, the United States Department of Justice indicted five Chinese military hackers on charges including computer hacking, identity theft, economic espionage, and trade secret theft from 2006 to 2014. The alleged actions affected six U.S.-based nuclear power, metal, and solar product companies. The indictment, filed May 1, 2014, alleges that the defendants obtained unauthorized access to trade secrets and internal communications of the affected companies for the benefit of Chinese companies, including state-owned enterprises. Some defendants allegedly hacked directly—stealing sensitive, nonpublic, and deliberative emails belonging to senior decision makers, as well as technical specifications, financial information, network credentials, and strategic information in corporate documents and emails—while others offered support through infrastructure management. Charges were brought under 18 U.S.C. §§1028, 1030, 1831, and 1832. (Source: Department of Justice Office of Public Affairs, http://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor).

Many companies choose not to publicly disclose or discuss these sorts of attacks or disruptions, which may go undiscovered for many months and often years. Even when attacks are discovered, breaches may not be reported to law enforcement or even to affected commercial partners. Questions about historical incidents during due diligence therefore should be open-ended but also very direct:

- Have you suffered thefts of confidential data (wherever stored)?
- Has your network suffered an intrusion?
- Did you retain outside experts to investigate?
- What is known about the attackers and the attack vector?
- What data do you suspect or know were taken?
- How long between the first known intrusion and discovery of the incident?
- Do you suspect or know whether the thief or intruder attempted or made fraudulent or competitive use of exfiltrated data?
- During the past three years, have you experienced an interruption or suspension of your computer system for any reason (not including downtime for planned maintenance) that exceeded four hours?

A buyer should assess a target's measures to prevent and detect insider threats, including whether basic protections are in place to identify and mitigate insider threats, such as the following:

- Pre-employment screening via dynamic interviews, background checks, and reference checking
- Workforce education on warning signs
- Internal network security measures such as website monitoring, blocking access to free (unauthorized) cloud-storage sites such as Dropbox, turning off USB drives
- Automated monitoring of Web, deep Web, or peer-to-peer network searching for leaked data.

Private and state actors have made use of denial of service attacks to disrupt the business of a company that meets with their disapproval (or as an extortion scheme). Material impact on ecommerce, on-line entertainment, email, and other critical systems are the result. An acquirer might reasonably ask:

- Has the target company evaluated its exposure to such attacks?
- What measures does it have in place to defend itself?
- How would it know if such an attack was occurring?
- Have any such attacks occurred?

Assessing cyber insurance

Finally, buyers should evaluate the extent to which cyber risks are mitigated by insurance coverage, including whether enhancements to the cyber program may be available post-closing. Most cyber insurance policies today cover the data breach and privacy crisis management expenses associated with complying with data breach notification laws. Those costs include the costs of expert legal, communications, and forensic advisors, benefits such as credit repair or monitoring to affected individuals, and even costs of responding to government investigations or paying fines. Cyber coverage is also widely available for extortion events, defacement of website, infringement, and network security events, even arising from theft of data on third-party systems or malicious acts by employees. Because of the volatility and variability of the cyber insurance market at this time, buyers should closely examine policies for what is covered, deductibles, coverage periods, and limits. Diligence experts should also evaluate post-closing opportunities to enhance the insurance program if significant unmitigated risks of third-party liabilities or direct expense from an attack have been identified.

Conclusion

If there was ever an era when minimizing or commoditizing assessment of cybersecurity risks in the M&A space was sensible, that time has surely passed. Expertise in assessing data-driven risks should be embedded on the front end of every transaction and tracked throughout the deal, so that deal terms, deal value, and post-closing opportunities to strengthen security can be considered against a fully developed factual picture of the target company's cyber readiness and exposure.

LATHAM & WATKINS LLP

Latham & Watkins LLP

555 Eleventh Street NW
Suite 1000
Washington, DC 20004-1304
Tel +1 202 637 2205
Web www.lw.com

JENNIFER ARCHIE

Partner
Email jennifer.archie@lw.com

Jennifer Archie is a litigation partner in the Washington, DC, office of Latham & Watkins with extensive experience investigating and responding to major cybersecurity and hacking events, advising clients from emerging companies to global enterprises across all market sectors in matters involving computer fraud and cybercrime, privacy/data security compliance and program management, advertising and marketing practices, information governance, consumer fraud, and trade secrets. Ms. Archie regularly supports Latham & Watkins' leading national and global M&A, private equity, and capital markets practices in identifying, evaluating and mitigating deal or company privacy and data security risks.