DATA-SECURITY PROBLEMS FOR SALE

CYBER RISK CHALLENGES AND THE M & A LANDSCAPE

Karen Painter Randall and Steven A. Kroll Connell Foley LLP

As of Summer 2016, more than 600 M&A transactions were announced, the total value of which is estimated to be $37.4 billion. Many of these M&A transactions involve a dependence on technology, connectivity, and networks. Jason Weinstein, former deputy assistant attorney general at the U.S. Department of Justice, summarized the issue of cybersecurity due diligence succinctly when he said: "When you buy a company, you're buying their data, and you could be buying their data security problems…" As a result, cyber risks must be evaluated right along with financial and legal due diligence considerations.

The importance of cybersecurity due diligence was recently brought to the forefront when it was revealed that at least 500 million Yahoo! Inc. user accounts were victims of a data security breach during an advanced stage of a proposed billion-dollar acquisition of the company by Verizon Communications Inc. The breach is reportedly expected to result in substantial delays to the deal closing, painstaking investigations, and, most significantly, a reduced purchase price. In fact, Verizon announced that it lowered its purchase price for Yahoo's core business by $350 million, down to $4.48 billion. The situation was recently compounded further when on December 14, 2016, Yahoo disclosed another record-breaking breach of more than one billion user accounts that occurred in August 2013.

The Verizon/Yahoo deal is not the first M&A transaction to hit the headlines from a data protection perspective. In the lead up to the acquisition of WhatsApp Inc. by Facebook Inc. in 2014, the proposed use and transfer of WhatsApp's user data to Facebook for targeted advertising and other purposes was publicly scrutinized by the U.S. Federal Trade Commission. Two years later, Facebook's processing of user data obtained from its WhatsApp messaging service has found itself back in the spotlight.

In a world filled with more sensitive personal information than ever before, data has become "the new oil" and a key business asset for almost all companies. This begs the question: what do companies need to know about the cybersecurity and data protection of a target company before entering into not only an M&A transaction, but any transaction involving the purchase and sale of an enterprise's assets?

The term "cybersecurity due diligence" has been defined as "the review of the governance, processes, and controls that are used to secure information assets." Such due diligence may exist between states, between non-state actors, such as private corporations, and between state and non-state actors.

Cybersecurity is even a global issue between countries as nations try to protect themselves in the age of constant data breaches.

There are a number of different types of cyber risk scenarios to consider when exploring M&A due diligence: First, and, probably the worst-case scenario, is an ongoing breach. This is where the target company is "owned" by an unknown attacker, and any sensitive data or intellectual property might already be gone. Additionally, a public relations nightmare is most likely looming. Second, is an unrevealed previous data security breach. This occurs when the target company suffered a breach in the past that is revealed to the acquiring company only after the purchase, such as in the case of the Verizon/Yahoo deal discussed already. Third, is a persistent intruder. This is where the target company is host to an attacker that maintains their presence in the network environment, watching and waiting, which will now make the acquiring company a host as well. Fourth, a disruption attack, or an incident where attackers destroy critical business systems, leak confidential data, hold companies for ransom, and taunt executives. Fifth, a "dirty environment" where the target company's internal system demonstrates a significant amount of common malware, which will need cleaning, improved protection and detection capabilities. Lastly, an inadequate security program. This is where the acquired company has systemic cybersecurity issues resulting from a weak or nonexistent data security program. Weak oversight and guidance will, over time, create vulnerabilities across many security areas that will take time to remediate.

Whether you serve in the role of in-house or outside counsel advising a corporate client in an M&A transaction, there are a number of steps to take to assess the cyber risk of another company. First, counsel must identify the important data assets or crown jewels. In particular, it is crucial to identify the most sensitive data, such as: private and confidential information, intellectual property, trade secrets, and other propriety information that cyber criminals are interested in stealing.

Second, counsel must determine how the data is stored in order to understand where it is located, who is responsible for it, and how the company is protecting it. Thus, counsel must ask questions such as, is the target company storing their own data or using a third-party contractor, such as a cloud provider? What security precautions are in place to monitor and protect the data? Who is responsible for the data in the event of a breach? Have there been any prior breaches and how were they responded to and remediated?

Third, counsel must review the internal data controls of a target company. This assessment includes reviewing the internal policies and procedures in place to prevent a data breach. For example, social engineering is a major cause of data breaches. What are the target company's protections against phishing attacks, or internal leaks, such as a disgruntled employee emailing private data or taking it home on a thumb drive and then selling it?

Fourth, counsel must identify any past security breaches. Past behavior is a predictor of the future, so it is critical to know if a target suffered a prior breach and how it responded to and remediated same. This includes reviewing the stability/adequacy of data response plans as well as post-breach remedial efforts.

Fifth, counsel must review breach response plans. Steps should be taken to ensure a specific crisis management plan is in place – and has been tested – for responding to a cyberattack. When such an incident occurs, the company needs to be prepared to respond to inquiries from its stockholders, customers, clients, vendors, the media, government regulators, and law enforcement officials. A well-reasoned response plan increases the likelihood a target company will successfully manage the public relations and reputation risks associated with a cyber incident.

Sixth, counsel must consider the need for specific cybersecurity deal terms. Based upon what may be discovered during the due diligence stage, counsel will need to re-evaluate whether the deal is still right for his/her client. If it is, counsel may need to include data and cybersecurity-related risk provisions in the purchase and sale agreement to address data vulnerabilities and mitigate any post-closing exposure.

Finally, counsel must assess the impact of a potential cybersecurity incident to an insurance policy or post-closing agreement. An acquiring company should work closely with its counsel to carefully review their cyber insurance policies to determine important issues, such as: whether coverage exists for business interruption; if pre-acquisition cyber incidents are excluded; whether the policyholder/buyer is required to update its software/computer systems to include the latest patches and security protection measures; whether the policyholder/buyer was required to perform pre-closing cybersecurity due diligence in order to collect under the policy; and whether the policyholder/buyer has coverage for cyber risks it inherits from the target post-closing.

Ultimately, in an era where personal data has become integral to many businesses, a company's security measures and preparedness for a data security breach can only increase the value of the business to a potential suitor. As recent headlines have demonstrated, acquiring companies cannot afford to be kept in the dark with regard to vulnerabilities related to cybersecurity. There is simply no longer an excuse for data protection due diligence to be overlooked or inadequately tailored to a target company's risk profile. Accordingly, data protection issues should be carefully assessed and handled at the outset and throughout the M&A process. Moreover, both counsel and their clients must be cognizant of the fact that strategic issues with data protection at their core may creep up at various stages of the acquisition deal, including during the development of an acquisition or approach strategy at the genesis of a deal, and through integration and transition strategy post-completion. Lastly, data protection issues do not vanish once the transaction is closed. Thus, wary buyers should continue to assess and review its own data protection compliance requirements with audits following the signing of the deal, or be prepared to face scrutiny.

Karen Painter Randall is a Complex Litigation Partner with Connell Foley LLP in Roseland, N.J., and chair of the firm's Data Security and Data Privacy and Professional Liability Practice Groups. She provides representation and advocacy services to professionals and businesses in a wide variety of complex litigation matters and is a veteran trial attorney in state and federal courts. Ms. Randall, vice chair of USLAW's Data Privacy & Security Practice Group and a former chair of USLAW's Professional Liability Group, is designated a Certified Civil Trial Attorney by the Supreme Court of New Jersey.

Steven A. Kroll is an Associate with Connell Foley LLP in Roseland, NJ. He is a member of the firm's Data Security and Data Privacy practice group. In addition to representing professionals in various areas, Mr. Kroll concentrates his practice in the areas of professional liability and employment law matters in both New Jersey and New York. Mr. Kroll received his J.D. from Rutgers-Newark School of Law in 2009, cum laude, and received the distinguished award of Order of the Coif.