CRAIN CONTENT STUDIO Cleveland

CRAIN'S CLEVELAND BUSINESS

ACG Cleveland SPECIAL ADVERTISING SECTION
CORPORATE GROWTH & M&A

Don't let a data breach derail the deal

Cybersecurity assessments critical in M&A

By TOD A. NORTHMAN and THOMAS R. PEPPARD JR.

The global cost of cybersecurity breaches in the business world is forecasted to exceed $2 trillion by 2019. The average cost of each data breach is more than $4 million and growing annually, according to a 2016 IBM-sponsored study. Of those businesses that participated in the study, 26% were likely to experience a cyberbreach in the next 24 months.


Northman


Peppard

Earlier this fall, Verizon signaled the need to re-evaluate its $4.8 billion bid to buy Yahoo! upon discovering a previously undisclosed Yahoo! data breach. With all of those cringe-worthy statistics in mind, cybersecurity due diligence should no longer be an afterthought to most buyers and their legal counsel.

For many buyers, the focus on business diligence ends once they get their arms around the usual suspects such as financials, process, personnel, customers and suppliers.

That is unfortunate, because the likelihood and significance of losses from cybersecurity breaches can be readily mitigated by well-designed due diligence. In addition, potential targets can enhance the value of their businesses by adopting robust cyber risk-management programs.

Buyers tend to evaluate a target's information technology system based on whether the technology is sufficient to conduct business. Those buyers also are most concerned about confirming that industry-specific data security certifications, such as payment card industry compliance, are in place.

Certification is important but insufficient. Target, Home Depot, and Yahoo! all were payment card industry-certified when their credit card systems were breached.

Failure to rigorously explore a target's cybersecurity plan is an expensive lost opportunity.

Valuable intelligence can be learned by modestly expanding the scope of review if knowledgeable advisers, both legal and technical, guide the investigation.

The goal is to evaluate the sophistication of the target's understanding of its data security risks, but the problem is that many don't even know where to begin. While certainly not comprehensive, these are some suggested lines of inquiry for buyers to get the ball rolling:

- Review the target's cybersecurity organizational structure. C-suite leadership should spearhead the effort. Stakeholders across the business functions (operations, treasury, legal, human resources, IT, risk management and audit) must participate. Alarm bells should go off if cybersecurity is the province of the IT department alone. Analyze the role of target's counsel in evaluating and complying with the regulatory and enforcement environment.
- Evaluate target's cybersecurity budget and consider its annual growth. Review the target's unaccomplished goals for cybersecurity.
- Study target's recovery plan, including the adequacy and reasonableness of its recovery points and time objectives. Consider when it was last reviewed and by whom.
- Assess how target exploits and protects its IT assets. Target should prioritize defending against the greatest threats to target's information, networks and systems.
- Investigate prior cyberbreaches. Consider what is known about the attackers, what information was taken and what use was made of it, and how long it took from the time of intrusion until detection.
- Analyze cybersecurity training programs for personnel. Review how frequently audits are performed. Human error causes 25% of cyber breaches in the U.S., behind malicious and criminal attacks (48%) and system glitches (27%).
- Determine if third-party business partners hold company-sensitive information or are given the ability to access the company's systems. Examine whether protections are in place to safeguard such information.
- Assess the adequacy of breach notification systems. The longer it takes to detect and address the breach, the greater the damage done.
- Evaluate the process for protecting the business' information from misappropriation by former employees. Buyers should also consider including express representations and warranties in the definitive purchase agreement relating to privacy, data protection and security (including any security breach notification requirements). This ensures compliance with applicable law, industry standards and the target's existing policies and procedures.

Having policies in place is the first battle, but compliance wins the war. The need for express representations and warranties is two-fold: to ensure the necessary information sharing and to make certain that there is an appropriate level of risk allocation between the buyer and seller.

Without understanding the target's data security policies, any prior or existing breaches, and how the target's plans and procedures can be retained (or replaced) going forward, there is no way for buyers to perform an educated assessment of the potential risk in a proposed transaction.

Tod A. Northman is counsel at Tucker Ellis LLP. He can be reached at tod.northman@tuckerellis.com. Thomas R. Peppard Jr. is counsel at Tucker Ellis LLP. He can be reached at thomas.peppard@tuckerellis.com.