Blogs
Book of Jargon® & Apps
Events
Presentations
Thought Leadership
Videos
Webcasts & Podcasts

YOU MIGHT ALSO BE INTERESTED IN

Data Privacy, Security & Cybercrime
Information Technology - Hardware, Software & Services
Internet & Digital Media
Mergers & Acquisitions
Technology Transactions

7 TIPS FOR CONDUCTING EFFECTIVE CYBERSECURITY DUE DILIGENCE IN M&A TRANSACTIONS

29 October 2015

CONTACTS

Jennifer C. Archie
Washington, D.C.
T +1.202.637.2205
jennifer.archie@lw.com
view bio

SHARE

Email Facebook
Google+ LinkedIn
Twitter

1. Start Early

Buyers should begin conducting cybersecurity risk assessments early in the engagement process. The target should be able to identify which information technology systems and data sets are key to the business and explain how the company protects them.

2. Tailor Diligence

Based on the information gleaned during the initial risk assessments, the buyer should tailor its diligence based on the type of information being handled, the industry, and how important information security is to the target's bottom line.

3. Assess Awareness

Does the target's management team have cross-functional awareness about cyber risk and the their security program? If so, this is a sign of a mature security program. A security program will not be effective if it exists in a silo inside the information technology department. All substantial stakeholder departments should be involved in cybersecurity risk management.

4. Ask the Experts

In order to accurately assess cyber readiness and potential liabilities, buyers should assemble deal teams that include subject matter experts. The deal team should be nimble and focus on the specific industry, as cybersecurity risks are highly variable across sectors.

5. Ensure Payment Card Industry Compliance

If the target accepts, processes, stores or handles cardholder payment data streams, buyers should pay special attention to compliance with the payment card industry data security standards (PCI DSS). When done correctly, PCI DSS compliance is costly and requires constant adaptation and optimization to new threats and standards.

6. Consider Other Risks

Payment and card security are not the only risks to be concerned about. Theft of trade secrets, state-sponsored espionage and cyber attacks that cripple corporate networks can be just as damaging to a target business. Buyers should ask questions about any historical incidents in these areas and assess the target's measures for preventing similar future breaches or attacks.

7. Consider Cyber Insurance

Buyers should evaluate which of the target's cyber risks will be mitigated by insurance coverage. Today, most cyber insurance policies cover a data breach and the crisis management expenses associated with complying with data breach notification laws.

Find Out More

For more information on conducting cybersecurity due diligence in

M&A transactions download Archie's chapter from *Navigating the Digital Age*, "Cybersecurity due diligence in M&A transactions: Tips for conducting a robust and meaningful process."