LAREDO & SMITH, LLP

IN BRIEF

A "Top Down" Approach to Managing Cyber Risk

There are few "hotter" topics in corporate boardrooms these days than understanding the risks from a cyber attack and the measures to thwart, or at least minimize the risk of, a cyber breach. Indeed, the consequences of a cyber breach can be severe, including loss of valuable intangible property, a drop in share price, disclosure and reporting obligations to the SEC and other agencies, and litigation against the company and its board of directors.

While it may be tempting to downplay or relegate the risk as primarily affecting companies with HIPAA concerns … think Anthem … or retailers handling consumer credit data … think TJ Maxx and Home Depot, the truth is that any organization that owns or handles confidential information, including proprietary, IP and other intangible assets, is at risk of being hacked. Contrary to popular belief, smaller organizations with less robust data security may be at greater risk of a cyber breach than a Fortune 100 company with the resources to make data security a top priority.

Not Just an "IT issue"

Unfortunately, many organizations assume that cyber security is an "IT issue" and relegate the responsibility to an overworked/understaffed IT group whose primary responsibility is to troubleshoot and make sure that the company's technologies work on a day-to-day basis. Research shows, and current best practices confirm, that in order to have an effective cyber security program, the responsibility to secure data must be "enterprise-wide," running from the board down to the rank and file employee. In other words, organizations need to take an integrated approach to managing and allocating cyber risk that includes

(continued on other side)

NEWSLETTER • JUNE 2016

Mark Smith traveled to Washington D.C. on behalf of the Boston Bar Association to meet with members of the Massachusetts Congressional delegation.

We welcome **Payal Salsburg** to the firm as an Associate. Payal focuses her practice in the areas of business litigation, e-discovery and cyber law.

Jessica Yau Conklin was quoted in a recent Massachusetts Lawyers Weekly article about the early success of her networking group, BANG (the Boston Associates' Networking Group).

Happy 4th of July!

We proudly celebrate our freedom in our great country!

LAREDO & SMITH, LLP

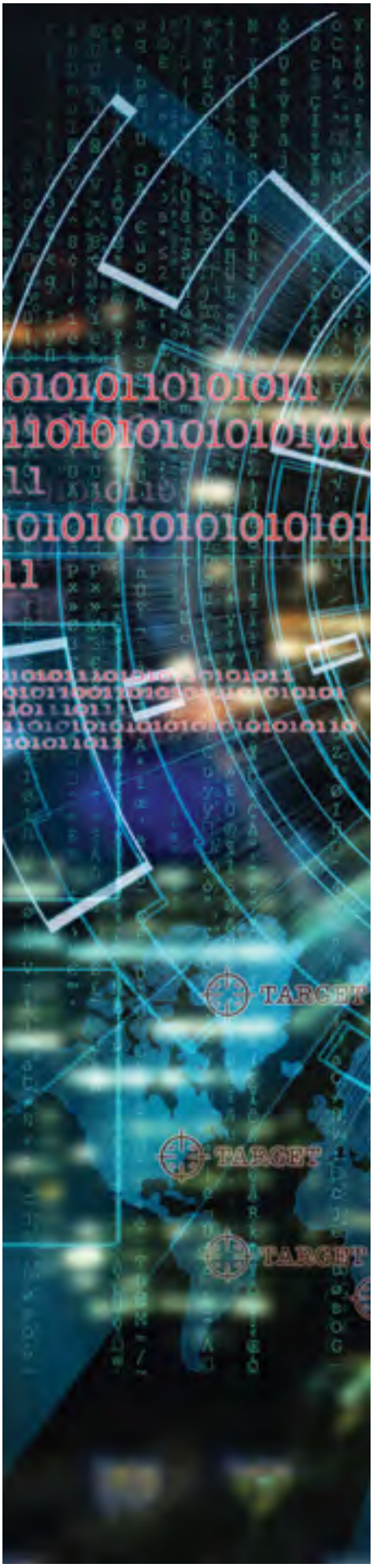
(continued from other side)

establishing a cross-departmental cyber risk management team consisting of business unit leaders from IT, legal, compliance, internal audit, finance and HR. This "cyber security committee" should meet regularly, develop and track metrics for evaluating program effectiveness, quantify the financial impact of the program, obtain adequate budget and resources, and periodically report to the board.

In addition to the organization's internal team, the board and senior management should have ongoing access to external cyber security experts who can advise on the strength and effectiveness of the program, including auditors, outside counsel and cyber security firms. Access to, and advice from, such experts will help the organization and its legal team defend the program in the event of a breach, as well as build shareholder confidence that leadership has taken appropriate measures to protect the company and its assets.

Last, but by no means least, because budgets for cyber security are finite and the focus needs to be on protecting critical assets, management must determine the level of risk the organization can tolerate and whether any portion should be transferred through cyber insurance. Current "cyber policies" usually provide coverage for (1) internal forensic investigations; (2) remedial measures, including costs for privacy notification and identity theft protection services; (3) business interruption and IT systems restoration costs; (4) third party claims, including costs of defense, settlement and judgment; and (5) enforcement actions, including defense costs, fines and penalties. However, because most cyber policies contain numerous exclusions, it is important to engage a knowledgeable insurance broker who can help select the right policy to address the organization's needs.

Though each organization's risk and approach to cyber security will no doubt vary depending on its size, culture and the nature of its critical assets, organizations serious about cyber security will ensure that the threat is addressed from the board down to the IT technician on an enterprise-wide basis.



101 Federal Street, Suite 650 | Boston, MA 02110 | 617-443-1100
www.laredosmith.com