How to talk to the board about security

(As published in the Wall Street Journal, CIO Journal, November 20, 2012)

Discussions about information security with the board of directors should highlight the most serious risks a business faces and the methods the organization is employing to manage them.

The surge in high-profile data breaches and cyber attacks that have occurred over the past five years has prompted many corporate boards to begin asking pointed questions about their companies' information security practices. They want to know: What are the odds our company will experience a damaging security breach, and what are we doing to prevent that from happening?

Consequently, CIOs and CISOs are increasingly being called upon to answer these questions during board meetings. The clarity of their responses can make or break their information security agendas, says Irfan Saif, a principal in the Security & Privacy practice of Deloitte & Touche LLP's Enterprise Risk Services business.

"Providing clear answers that articulate the imminent security and privacy threats your organization and the broader marketplace face and that speak to existing and planned risk mitigation strategies can win board members' confidence and help advance the security agenda," he says. "By contrast, overly detailed answers that delve into day-to-day security operations may overwhelm or frustrate the board."

It's not uncommon for those CIOs and CISOs, who've never previously had to report to the board on information security issues, to make the mistake of providing too much information, adds Saif.

"They tend to want to demonstrate a depth of coverage, so they present 50 metrics showing different risk dimensions," he says, "but that distracts everyone from the few critical risk indicators that are most important to the business."

Saif outlines three core messages CIOs and CISOs should communicate to the board:

1. **Shortlist the top four to six cyber risks your company** faces and the risk indicators that signal your company's level of exposure to them. The information security risks a company faces may include intellectual property theft, a data breach that compromises sensitive customer information, or financial and third-party fraud. The indicators CIOs identify to help assess their companies' risk exposure may include, for example, the number of monthly attempts to access the corporate network from countries that are known sponsors of cyber espionage and intellectual property theft or quarterly revenue losses associated with customer data leakage incidents. These primary risk indicators are important to communicate to the board because they help to illustrate the strengths and weaknesses of a company's overall security posture.

2. **Identify whether your key risk indicators are trending up, down, or remaining flat quarter over quarter.** If your risk indicators are moving, explain what might be causing those shifts. For example, says Saif, if you notice spikes in cyber attacks during the weeks or months leading up to product launches, you should point out such correlations to the board. "The board should be aware of cyber threat trends that tie to business performance and the cyclical nature of information security risk," he says.

3. **Explain how the company is managing security risks and keeping them within acceptable limits.** For example, if unauthorized distribution of sensitive corporate information is a high risk for your company, you may need to explain at a high level the technologies and processes the company has in place to monitor information sent both inside and outside of your organization, detect suspicious communications, and restrict their transmission until legitimacy is verified. If unauthorized third-party access to sensitive information poses a threat, you can describe your company's stringent security assessment processes for dealing with third-party vendors.

Saif acknowledges that communicating with the board about information security is complicated by the fact that a typical, two-day board meeting may devote just 15 minutes to the topic. That's why it's essential for CIOs and CISOs to present the few risk indicators that are most important for the board to understand and give them time to ask questions. Another leading practice he recommends is to provide concise briefings to the board before meetings that serve to focus their attention on critical information security concerns, as well as potential mitigation plans.

Finally, Saif advises CIOs and CISOs to present an objective view of what the company is doing well in addition to its critical vulnerabilities. He notes that board meetings are an opportune time for CIOs and CISOs to be candid about the security implications of various staffing, budget, and prioritization decisions on other in-flight and planned business and IT initiatives.

"It does no one any good to present a message to the board that's skewed positively or negatively," says Saif. "It's important for the board to get a balanced view of the company's security and risk posture. They need to understand as transparently as possible what the risks are and what the business is doing about them so that they can ask the right questions to govern the process."

Irfan Saif is a Principal at Deloitte & Touche LLP, and specializes in aspects of security and privacy, including cloud computing, identity access management, and focuses on the Technology, Media & Entertainment and Telecom industry.

Please visit the Center pages on
http://www.deloitte.com/us/securityandprivacysolutions
to learn more about this and other topics of interest on security and privacy.

For more information, write us at
ussecurityandprivacy@deloitte.com

Contacts

Rhoda Woo
National Managing Director
Security & Privacy
Deloitte & Touche LLP
+1 212 436 3388
rwoo@deloitte.com

Irfan Saif
AERS Principal
Deloitte & Touche LLP
+1 408 704 4109
isaif@deloitte.com