Cybersecurity should be front and center on your board’s agenda

November 5, 2015 by Stuart R. Levine, Stuart Levine & Associates LLC

Data security and intellectual property protection affect all levels of business activity. The nature of the threat is formidable because of its complexity and the speed of evolution of types of attacks. A number of high-profile cyber attacks have caused boards of directors to deal with security issues that they once left to technology experts. Now it is imperative that boards be well equipped to handle the situation. One misstep can cause untold costs from compromised data, loss of customer trust, diminished competitive position, fines, lawsuits, and damaged reputation. While the approaches taken by individual boards will vary, attentiveness to the problem by every board is a must.

Still, too many boards face a risky combination of lack of knowledge and lack of information. A recent study by The National Association of Corporate Directors illustrates the problem. The “Public Company Governance Survey” reported that 87% of respondents thought that their board needed improvement in its knowledge of information technology, including security. Moreover, this concern extends to management. Deloitte found that only 10% of 101 CFOs surveyed earlier this year, most at companies with greater than $1 billion in revenues, said they were well prepared for a major cybersecurity crisis, while almost 25% were insufficiently prepared.

Board members and management alike can be well served by educational programs designed to address this gap. Existing advisors, especially those with industry-wide and multi-company experience, such as independent auditors and outside counsel, can provide briefings. Other experts, like cyber-security firms, government agencies and industry associations can also provide much needed learning. Some boards consider recruiting directors with cybersecurity expertise, when they seek to balance required skill sets.

Boards must effectively oversee and approve management’s cybersecurity risk planning. They need current and complete information about the company’s overall data protection program. Yet, a recent NACD survey found that only 12 percent of board members said they frequently receive briefings on cyber-preparedness. Over 60 percent of boards did not regularly receive such reports, and 26 percent rarely or never received them. Moreover, senior management, which is charged with reporting cyber-risk issues to the board, must make certain that they are adequately informed. The Ponemon Institute, which researches cybersecurity, reported that when it asked 600 IT professionals about their practices, 60 percent generally did not report cyber-risks until they believed them to be urgent. At that point, the problem is often more difficult to handle.

Management must have a data protection team that is properly structured to be most effective. The team leader should have cross-departmental authority, such as the CFO, COO or Chief Risk Officer. The cross-departmental senior leadership approach signals that data security and IP protection are critical as this impacts the whole organization. It is not just a technology issue involving the IT cost center. Our hyper-connected world poses governance and oversight challenges for boards. Regardless of the industry or size, every organization is truly vulnerable to threats to its intellectual property and data. Boards in their oversight capacity and senior management in its leadership role must be prepared.