

Cyber security: IT issue or board issue?

The plaintiff's bar is aiming right at the top when there's a breach, so take these actions to minimize your risk.

BY TRACEY VISPOLI

“WHERE WAS the board?” More and more, this is the question being posed today as an increasing number of companies face a cyber security meltdown in the form of a security breach and/or stolen personally identifiable customer information.

But is cyber risk really a board issue? Isn't computer security the jurisdiction of the IT department?

The answer, increasingly, is that cyber security is the responsibility of the board. Consider this possible cyber breach scenario:

A company discovers its computer systems were breached four months earlier. The company has no response plan for the mounting crisis. Within days, the enormity of the breach becomes clearer: The personal information of at least 500,000 customers — in all 50 states — may have been stolen. Under state privacy notification laws the company must pay to notify

each customer about the potential loss of their personal information, and the cost of notification could run as high as \$197 per customer. The first media stories appear and, with no response plan, the company is unsure how to reply — management decides not to comment. As the days pass, the number of affected customers grows and surpasses one million. Nervous shareholders begin a selloff and the company stock price slides. Barely two weeks after the security breach is discovered, the first

shareholder lawsuit hits, alleging mismanagement and breach of fiduciary duty by the board, and seeking millions of dollars in damages. In addition, the Federal Trade Commission informs the company it wants to investigate possible e-commerce violations.

Two recent cases demonstrate the increasing risk of a cyber security breach and the potential cost to the company:

- In early 2007, TJX Companies Inc. reported the theft of 45.6 million credit- and debit-card account numbers (later revised to more than 100 million). Thirty days after TJX reported the theft, bankers' groups, representing nearly 300 banks, sued the retailer for their members' card replacement costs. In December, TJX offered to pay a \$40.9 million settlement.

- This year, the grocery store chain Hannaford Bros. Co. announced that millions of credit- and debit-card numbers were stolen by data

thieves. Two days after the announcement, Hannaford was hit with the first class-action lawsuit. A second class-action lawsuit was filed the very next day.

The difference in the timing of the two lawsuits — 30 days for the former suit versus two days for the latter one — is instructive. The quickened pace for bringing lawsuits suggests that the plaintiff's bar is gaining confidence it can recover significant dollars for plaintiffs in cyber breach cases — at the expense of the board of directors.



Tracey Vispoli is a vice president and global financial fidelity and cyber security manager for the Chubb Group of Insurance Companies (www.chubb.com).

What can a board member do? Most important, remember that responsibility for cyber liability is more commonly being placed with board members — today, when a network security breach causes harm, plaintiff's attorneys are aiming straight for the top of the organization for recovery.

With this in mind, the board should consult with general counsel to ensure it is taking the proper precautions to minimize cyber liability exposure. The following actions may also help the board minimize corporate risk:

- Contemplate how a cyber crisis could play out in your company. Identify weaknesses in security and response systems and direct management to strengthen them.

- Ensure that someone has responsibility for cyber security, including compliance with the FTC's "pre-warning" requirements.

- Get an annual update from the company's chief information officer or chief risk officer on the company's computer security policy and plan. Such a plan should center on the company's IT philosophy and security culture, include a thorough inventory of the critical information under the company's control (e.g., private financial and medical information, trade secrets, competitive information), include insurance protection, and be tested.

- Don't be satisfied until you are comfortable the company is endeavoring to achieve government-mandated standard levels of compliance.

- Be assured that the company has assigned adequate resources for system security. Look at industry benchmarks to determine if the company's security expenditures are in line with other businesses like yours.

When it comes to computer security, you don't want to have to respond to questions regarding the whereabouts of the board in the event of a security breach. The time to proactively head off potential cyber disaster scenarios is now. ■

The author can be contacted at tvispoli@chubb.com.