



Taking Cover

Directors and officers respond to the growing threat of cyber attacks.

by Lori Chordas

In 2005 and 2006, hackers broke into the TJX Companies' systems and stole information from 45 million to more than 94 million credit cards and debit cards used in subsidiaries of the Massachusetts-based retailing group. The company is a leading off-price retailer of apparel and home fashions in the United States and worldwide whose off-price concepts include stores such as T.J. Maxx, Marshalls, HomeGoods and A.J. Wright.

Not only did the corporation and its customers suffer a big loss, but TJX also was sued and some individuals chastised the company's management team for not safeguarding its information.

In May, various news articles reported that TJX Cos. fired an employee after he left posts in an online forum that made claims about security practices at the T.J. Maxx store where he worked. Nick Benson said in an e-mail interview that lax security allowed employees to use blank passwords to log onto company servers. While the University of Kansas student, who goes by the

name Cryptic Mauler online, repeatedly brought security issues to the attention of several store managers, he said he was unaware of any changes to resolve those issues. Several months later, Benson was fired after managers said he disclosed confidential company information online in a Web site dedicated to Web application security.

Also in May, Pfizer Inc. reported that an encrypted laptop, as well as an unencrypted flash drive containing personal information about approximately 13,000 of its employees, was stolen from an employee's car. While the company said no Social Security numbers were on the unencrypted flash drive, it did contain names, home addresses, home telephone numbers, employee identification numbers, positions and salary information, including information from various Pfizer divisions that employ more than 5,000 individuals in Connecticut.

These are just two of a growing number of recent cyber-related incidents that have organizations' upper

► **State of the Market:** Cyber attacks are being unleashed faster than ever.

► **What's the Problem:** Directors and officers may bear some responsibility for loss to their companies.

► **What's Being Done:** Risk managers play an integral role in keeping executive management teams apprised of security measures and taking appropriate actions.

management executives scrambling for ways to protect themselves and their companies.

Cyber risks have a wide range, from copyright and patent infringement to data sabotage. They also may include network security failures; lost information assets; cyber extortion; libel, slander and defamation; and damages from viruses, worms and Trojan horses. Internal attacks also are on the rise.

Results can be devastating. Companies may face loss of customers, damage to their reputations and class-action lawsuits.

As for the devastating financial toll, privacy and information management research firm Ponemon Institute estimates the average total data breach

per-incident costs in 2007 at \$6.3 million and the cost of an event at about \$197 per compromised record.

Management on Alert

“Along with the growing threat, the vulnerability of directors and officers to the consequences of cyber attacks also is real,” said Donald Light, a senior analyst in international strategy consultancy Celent’s insurance practice.

That’s putting much pressure on companies’ management teams, added Tom Sheffield, technical director for global insurance brokerage Aon Corp. He said directors and officers may be the next target for lawsuits by shareholders wanting to hold management responsible for losses to companies and shareholders.

“If [directors and officers] haven’t taken the right precautions to prepare, respond and finance the cost of an event, they may find themselves exposed because they mismanaged the company,” said Jennifer O’Neill, senior vice president and D&O product manager at AIG Executive Liability.

Incidents such as what happened at TJX are a wake-up call to get “people to begin looking at this potential liability,” said Brian Thornton, vice president of technology, media and telecom underwriting for specialist insurer Hiscox. “It’s a threat that will continue to grow as more organizations go digital and use data in different ways.”

Taking Action

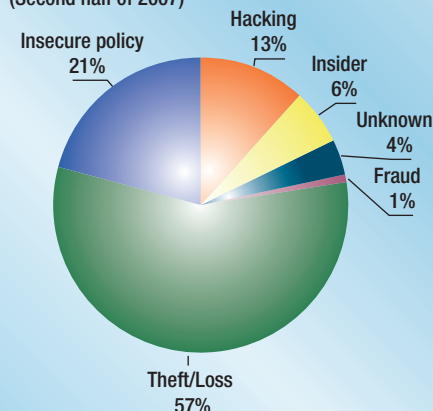
So, what can directors and officers do to protect themselves and their companies?

The most obvious step begins with putting adequate security protection measures in place. According to an IBM survey, 73% of CIOs responded to the threat of cyber crime by upgrading their anti-virus software, 69% upgraded their firewalls, two-thirds implemented intrusion detection or prevention technologies and 53% put patch management systems on their networks.

But as corporate America gets smarter about cyber attacks, so do criminals. Therefore, management teams must go beyond just the basic

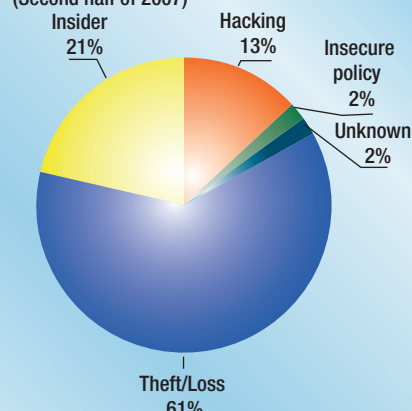
Causes of Data Breaches

(Second half of 2007)



Causes of Identity Theft

(Second half of 2007)



Sources: Attrition.org; Symantec

security measures, said Tracey Vispoli, vice president and global cyber solutions manager and the worldwide manager of financial liability insurance for financial institutions for the Chubb Group of Insurance Cos.

“All C-level executives need to be routinely thinking about security, evaluating trends and potential exposures,” she said. “It’s important that management begins from the highest level defining what their responsibilities are.”

Not only that, directors have to develop and regularly test strong IT security defenses and business continuity plans, Sheffield added.

“They also should increase awareness among their boards to create a security culture with all departments and employees. And, they have to determine how they’ll respond to the risk in the first place. Insurance is only one component of that,” he said.

Products also are designed to help. American International Group’s AIG netAdvantage provides security and privacy coverage. It includes Internet-media liability coverage, security and privacy liability, and crisis management, which includes hiring an emergency public relations team, notifying affected customers, and monitoring credit.

“Directors and officers also need to have an understanding of the range of threats,” said Light. “For instance, a board of directors might need to be briefed annually, while a CIO may require a monthly or quarterly conversation with the company’s chief security officer.”

And, he added, “the board should understand the inherent risks associated with a company’s technology platform in how it receives, transmits and stores electronic information.”

Getting the Job Done

Are directors and officers aware of their potential liabilities stemming from cyber breaches and threats?

That depends, said Light. “The issue has clearly moved up to a higher position on senior officers’ agendas, depending on how many headlines they read and how serious they are. But has it been discussed in enough depth and updated regularly? That’s where the picture has been much more mixed.”

Vispoli is skeptical that many directors and officers are fully aware of what exposure and reputational damages they might face from a security breach.

“That’s unfortunate because the threat is real,” said AIG’s O’Neill. “It’s not a matter of if a company will have a data breach, but rather when that will occur.”

Sheffield is more optimistic that management teams are “better understanding more about technology. More boards now are having discussions about disaster recovery, putting together comprehensive plans and installing virus protection software, and doing things on the front end.”

The regulatory environment also is changing. O’Neill said 39 states and the District of Columbia now have a patchwork of privacy and consumer



“All C-level executives need to be routinely thinking about security, evaluating trends and potential exposures.”

—Tracey Vispoli,
Chubb Group of Insurance Cos.

notification laws in which companies must abide.

Vispoli said the 2002 Sarbanes-Oxley Act also created some changes. “Since the fiduciary duties of board directors and corporate officers require them to evaluate and maintain a safe control environment, they’re responsible for seeing that the organization regularly evaluates its position on cyber security in the same way it analyzes other risks.”

But, the act isn’t specific about what companies need to do to adequately discharge those responsibilities, said Mark Silvestri, CNA NetProtect product line manager. NetProtect offers first- and third-party cyber risk coverage for various exposures. “We’re now seeing an emerging trend of enactment of expanded statute and regulation that’s trying to refine that criteria for adequately protecting against cyber risks.”

He said nearly 40% of breaches result from a third-party to whom a company entrusts its information. “That raises the [question] of whether

or not directors have done sufficient due diligence with any third-party they conduct business with and for whom they may be vicariously liable.”

Despite growing publicity, many cases get lost under the radar, said Thornton. “There are many situations where tens of thousands of identities are stolen. They don’t make the headlines but they really add up in the industry and take a toll on companies.”

While companies step up efforts, “no one yet has the solution,” said Sheffield. “We’re trying to get them to rethink how their policy applies to the situation and we seek ways for our clients—the purchasers of insurance—to drive the product more than in the past rather than allowing insurers to dictate what they’re comfortable with.”

Policy Protection

“Directors and officers have two options: Reserve against contingency or transfer the risk through insurance,” said CNA’s Silvestri.

“This is certainly on our radar screen from an underwriting perspective,”

said Thor Beveridge, vice president of underwriting—corporate governance for CNA. “The biggest issue facing directors and officers today is failure to maintain a controlled environment.

“But, it’s a gray area in underwriting around what companies are doing,” he said. “The biggest issue we look at is whether directors are being proactive in their approach toward cyber risk exposure. We ask boards if they’ve looked at, reviewed and updated internal controls, and hired a third-party consultant to examine the controls and report back any weaknesses to the board.”

How can insurance help? “That depends on the types of allegations brought forth,” Beveridge said. “If it was a breach of their fiduciary duty in maintaining a controlled environment, that’s something a D&O policy would likely respond to. But there are some exclusions in the policy, although nothing specifically related to cyber risks.”

Some of those exclusions may include bodily injury and property damage, emotional distress, and errors and omissions, said O’Neill.

She said most claims generally are brought against a company, not against individual executives. “In those cases, our standard policy only provides coverage for the entity for security claims. So, if a security claim arises out of that particular issue there may or may not be coverage

Managing Risks

A big part of companies’ cyber security efforts lies with risk management. “Companies want to have proper controls and processes in place to prevent an attack and constantly need to think about risk financing and how they’d pay for an event. That’s really a complete risk management function,” said Jennifer O’Neill, senior vice president and D&O product manager at AIG Executive Liability.

“Risk management is an all-encompassing role and shouldn’t be done in a silo,” said Tracey Vispoli, vice president and global cyber solutions manager and worldwide manager of financial liability insurance for financial institutions for the Chubb Group of Insurance Cos. “In some organizations, that means securing insurance for the company; for others, it’s taking an operational risk perspective. Risk managers are in the perfect position to

inventory and assign a probability and value on that.”

Chubb publishes a loss control handbook for risk managers that highlights various information security exposures and guidelines on how to protect their organizations. “Also, when we underwrite risks we walk through a network security audit tool that insureds complete online. They get scored and risk is modeled to show them areas of adequacy and deficiency,” she said.



Thornton

Hiscox helps risk managers explain to their boards the importance of security, said Brian Thornton, vice president of technology, media and telecom underwriting for specialist insurer Hiscox. “We offer them learning resources, put them in touch with vendors to perform security assessments, and offer an incident hot line where companies can call in if they fall victim to a breach.”

depending upon whether there's an exclusion in the policy."

Some changes are needed, said Thornton. "Currently, most insurance products that really provide coverage to companies are based on first-party losses. They'll step in and pay to get systems up and running and for lost time when a system is down. But they don't do a good job in dealing with resulting liability that directors and officers face. Our push now is to begin answering some of those questions."

Aon is currently reevaluating the policy language to help protect directors. "We're looking at how to broaden the policy to include both first- and third-party losses, and have considered different ways to describe the losses to companies," Sheffield



Directors have to develop and regularly test strong IT security defenses and business continuity plans.

—Tom Sheffield,
Aon Corp.

backstop. That, at least, gives directors some peace of mind that they're effectively managing the risk. I don't know that the D&O policies will provide adequate first-party and third-party coverage for those types of losses."

Also gaining traction in the market are cyber liability policies. Chubb began offering the coverage in 2001.

"Many organizations such as hospitals and retail companies are frequent

That leaves directors and officers in harm's way. "There will be more litigation coming from plaintiffs attorneys as they get better making claims and receiving damages," she said.

But management teams are starting to sit up and take notice. "The more boards of directors are dependent on technology, the more they'll ask questions of risk managers and outside vendors on whether their companies are adequately protected," said Sheffield. "That provides a real opportunity for the insurance industry to come up with products to answer that call for help."

He's concerned, however, the industry will always be a step behind. "Hackers will always be ahead of the curve because they spend more time dreaming up attacks. The question is how close is a company to [moving into] first place...I'm not convinced we're there yet." **BR**



"The board should understand the inherent risks associated with a company's technology platform in how it receives, transmits and stores electronic information."

—Donald Light,
Celent

said. "For example, we have focused on some approaches used historically in the Standard Form 24 for fidelity bonds. That form traditionally provided cover for losses stemming from employee dishonesty. Since some cyber attacks are from within, it makes some sense to look at traditional tools to measure and protect against loss."

Thornton now sees growing interest in privacy and network security policies on a stand-alone basis. "Brokers are recommending something from a D&O perspective because if there's a loss, at least they've addressed the privacy exposure from a risk management standpoint, along with purchasing an insurance policy as a

targets of cyber attacks. Language in the policy doesn't protect executives but protects the entity that may have a lawsuit brought on by consumers for the company's failure to provide adequate protection or systems' security of personal identifiable information," said Vispoli.

But, Thornton said, cyber policies "are kind of a generic term and carriers are adopting privacy policies that will cover not only a network security breach but also non-electronic losses, such as a lost laptop."

Racing Ahead

The threat of cyber attacks isn't likely to go away anytime soon, said AIG's O'Neill.

Learn More



American International Group

A.M. Best Company # 05953

Distribution: Global, national, regional and local brokers

Chubb Group of Insurance Cos.

A.M. Best Company # 00012

Distribution: Independent agents and brokers

CNA Insurance Cos.

A.M. Best Company # 18313

Distribution: Agents and brokers

Hiscox Insurance Group

A.M. Best Company # 25054

Distribution: Wholesale and specialized brokers

For ratings and other financial strength information visit www.ambest.com.



Watch a video about this article on bestreview.com/videos