

# RISK & INSURANCE®

Emerging Strategies for Risk



**DONNA PATCHE**, a victim of identity theft, talks about the issue in Santa Maria, Calif., in 2005. California has passed a law requiring companies to tell consumers when their data has been compromised.

## ● RISK MANAGEMENT

# Stealing Data the Old-Fashioned Way

**A recent rash of laptop thefts is a reminder that security breaches are not just the result of “cybercrime.”** BY JIM WEST

Security breaches have become a major concern for most businesses and for technology vendors in particular. Just in recent months, Hotels.com acknowledged

the theft of a laptop computer loaded with unencrypted data from a car belonging to an employee of Ernst & Young Global, the travel Web site’s auditor. The laptop

contained credit card numbers for nearly a quarter of a million customers. In a similar case earlier this year, Fidelity Investments lost sensitive data on nearly 200,000 Hewlett-Packard Co. employees.

Even the federal government has fallen victim to this problem. The U.S. Department of Veterans Affairs said in May that the theft of a laptop and external hard drive during a burglary at the home of a VA analyst meant the loss of data including names, Social Security numbers and addresses belonging to more than 26 million veterans. Fortunately, that laptop was recovered, information intact, in late June.

These incidents—and many more like them—follow a year that experts say was the worst ever for reported security breaches. The watershed was the ChoicePoint incident in February 2005, when hackers infiltrated one of the nation’s largest collectors of consumer information and put some 145,000 accounts at risk of identity theft. Since then, more than 88 million records containing sensitive personal information have been involved in security breaches, according to Privacy Rights Clearinghouse, a San Diego-based consumer rights group. The 2005 FBI Computer Crime Survey found that nearly nine out of 10 public and private organizations in the United States have been victims of some kind of computer security incident.

The growing problem of security breaches has led to the enactment of laws, as well as a great deal of discussion about possible legislation. The 25-nation European Union, for one, has issued directives on privacy. Also, at least 23 U.S. states have enacted security-breach notification laws that require firms to alert individuals when these incidents occur.

## **SIMPLY DATA THEFT**

Not long ago, the focus of security breach was on the Internet, with businesses working to tighten the security of their Web sites against theft of information, money and identities. But many of the latest, highly publicized security breaches had nothing to do with the Internet. Rather, they involved

the storing of sensitive and confidential information simply in electronic form.

No matter what business they're in—from hospitals to financial institutions to retailers—organizations that focus solely on their cyberexposures are not fully protecting themselves. This becomes clear when considering that security breaches can arise from four underlying causes:

- Performance or service failure, which occurs when an organization fails to prevent unauthorized access or unauthorized use of data.
- Hacker attacks directed at an organization or the Internet.
- Rogue employees who act to intentionally damage computer systems or data, or steal assets.
- Mistakes that unintentionally result in the disclosure of data.

The consequences of a security breach can be far-reaching for businesses, including lost income, privacy lawsuits, theft of personal and proprietary business assets, and contractual duties owed to others.

Consider the settlement earlier this year between the Federal Trade Commission and CardSystems and its successor, Solidus Networks. In 2005, the credit-card-processing company's computer system was breached by data thieves, compromising 40 million accounts. The settlement requires CardSystems to designate an employee or employees to coordinate and be accountable for the information security program.

The company must also identify internal and external risks to the

**INSURANCE CAN  
HELP PROTECT TECH  
COMPANIES FROM  
THE POTENTIAL  
FINANCIAL DAMAGE  
... BUT ONLY IF THE  
INSURER PROVIDES AN  
INTEGRATED APPROACH  
THAT INCLUDES MORE  
THAN JUST "CYBER"  
INSURANCE.**

—Jim West, senior vice president,  
Chubb & Son

security, confidentiality and integrity of its consumer information that could result in unauthorized disclosure, misuse, loss, alteration or destruction of such information, as well as assess the safeguards in place to control these risks.

CardSystems must design and implement reasonable safeguards to control the risks identified through risk assessment, and regularly test or monitor the effectiveness of the safeguards. Then it must evaluate and adjust their information security program in light of the results of testing and monitoring, any material changes to their operations or business arrangements, or any other circumstances that may have an impact on the effectiveness of the program.

These requirements won't end anytime soon either. CardSystems must obtain a biennial security audit for the next 20 years. CardSystems also faces potential liability in the millions of dollars for losses related to the breach, the FTC noted.

In light of this and other exposures, organizations are not only turning to their technology vendors for solutions, but also holding them accountable. Whether involved in hardware manufacturing, software development or providing technology/networking services, no technology company is immune. Tech companies offering security products or solutions have the greatest potential exposure. But today, all technology companies are exposed, because security is a feature in virtually all technology products or services.

Until recently, the burden was on the end user of technology to protect confidential data. Now, there are increasing indications that the onus will be on technology companies if security breaches occur because their products have not properly protected the data. This change is already evident in contracts. Two years ago, it was rare to see a specific reference to security in a contract with a technology vendor unless it involved someone tied to security.

But a year ago, these agreements began mentioning the contractual obligation of the technology vendor to keep data secure. Now this has become universal in contracts as the end user makes the tech company responsible for securing information.

Any technology provider that sells a product or service that includes a security

feature faces the risk of being sued. Failure to protect personal and confidential information creates legal exposures, ranging from contractual duties owed to customers and consumer privacy lawsuits to possible tort-style product-liability lawsuits.

Tech companies should be mindful of the functioning of the software, as well as the security of the software application, during the product development phase. They also should ensure that salespeople do not overstate the level of security. In contract management, a technology firm must expect to be pressed on security issues.

This enterprisewide approach should be taken at the most senior level to make certain that all aspects are reviewed in the context of security. If that fails to happen, technology companies are bound to end up assuming more liability potential than they are ready to handle.

### **MORE THAN A CYBERRISK**

Insurance can help protect tech companies from the potential financial damage of a security breach, but only if the insurer provides an integrated approach that includes more than just "cyber" insurance. Some carriers offer Internet liability policies, cyberliability policies, or even privacy and information-security policies. While these may do a good job in handling security-breach exposures, they are far too specific to deal with all of a technology firm's exposures.

Therefore, a customer who buys one of these activity-based policies is ill-served because it is not responsive to other causes of loss, which can range from failure to comply with contract terms or failure to deliver a project on time, to a product defect that impedes effective operation or misrepresentation in marketing materials regarding product capability.

The best and most complete protection comes only in the form of an integrated, enterprisewide approach that incorporates insurance products and services, addressing property, business income/extra expense, crime, malicious programming, general liability, intellectual-property liability, and errors and omissions exposures.

---

**JIM WEST** is senior vice president, Chubb & Son, and manager of Chubb's Information and Network Technology segment. He can be reached at [riskletters@lrp.com](mailto:riskletters@lrp.com).



**Chubb Group of Insurance Companies**  
Whitehouse Station, New Jersey 08889  
[www.chubb.com](http://www.chubb.com)