www.propertyandcasualtyinsurancenews.com P&C
National Underwriter
THE LEADER IN PROPERTY & CASUALTY NEWS

SECURITY & CYBER RISKS

Human Error, Lax Security Procedures Open Data Breaches, Create Liabilities

Better risk management, software solutions can help secure porous IT systems

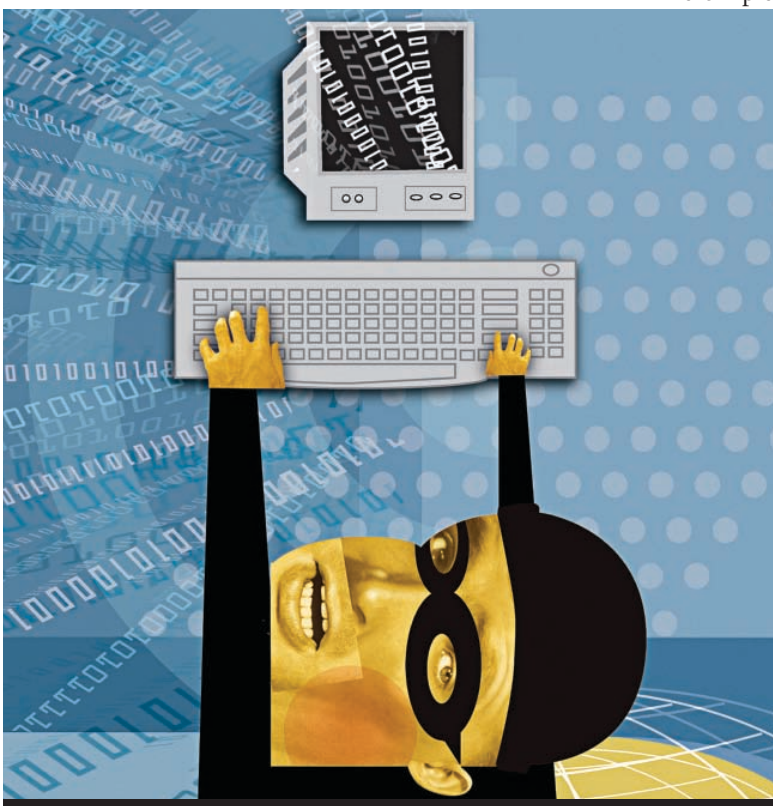
BY BOB DITMORE

WHAT IF A PROFESSOR LOSES HIS LAPTOP containing sensitive information about students while he is on vacation in Africa? Or a company's internal database with private employee information is inadvertently exposed to the world on an external Web site?

What happens if backup computer tapes are lost en route to an offsite storage site and it is unclear whether the information on them is protected by encryption? Or what if, by mistake, a company sends out a bill to one customer that includes private information about other customers?

Contrary to what many might think, the common thread among these data breaches is not the hackers (outsiders who break into your computer system) and phishers (e-mail con artists who try to trick you into supplying private information) that people worry about when they think of stolen data.

Actually, the common problem is a lack of adequate risk management—most often lax company procedures and human error.



STANDARD SECURITY STEPS such as changing passwords, erecting firewalls and encrypting sensitive data are no longer adequate to protecting computer systems.

These types of incidents have always been far more frequent than anyone likes to admit, but they are increasingly coming to our attention because of laws and regulations that require companies to notify people who are potentially affected when data goes astray.

As they fall under increasing regulatory scrutiny, companies need to focus on data security to avoid not only the cost of cleaning up security breaches but also the loss of reputation and trust that can affect future business growth.

The simple approaches of the past—requiring employees to change passwords frequently, relying on firewalls to keep out hackers and encrypting sensitive data—are no longer enough.

Fortunately, as the threat of data loss has grown more complex, the technology tools designed to protect information have become increasingly more sophisticated.

Combined with rigorous risk management policies and procedures, these tools can help companies avoid costly data breaches.

THREAT FROM WITHIN

Three trends are driving increasing efforts to protect private data.

- First, more data about people is being collected than ever. With our information-intense economy and the continuing development of technology networks, personal data is housed by almost every business and government

Bob Ditmore is senior vice president of global technology for Hartford-based Travelers. He can be reached at bditmore@travelers.com.

organization that touches our lives.

- Second, the portability of equipment is an increasingly challenging issue. Information no longer becomes mobile just on laptops but also on external hard drives, tiny flash drives and even cell phones.
- Third, regulatory attempts to force companies and organizations to take security seriously are growing. Today, more than 35 states require the holders of information to alert people whose data has been exposed.

While most people believe the biggest threats to their privacy are evil computer hackers, the truth is usually far more mundane. In many cases, problems begin with an organization's policy that backfires or an employee who makes a mistake.

The solution to data breaches boils down to establishing smart policies, training employees on proper procedures, and then following up with frequent monitoring and enforcement.

Today's sophisticated data security software can help an organization by "fingerprinting" sensitive data so it can be detected as it moves through and out of a system. Such software can also perform real-time scanning and analysis to detect unusual patterns of data use. And it can store events related to critical information in a searchable database to help with post-incident analysis if data is lost.

Today's technology has opened the door to new risks, but it has also supplied tools to address that risk. However, in the end, common sense is the best guide to protecting private data. Among the steps you can take:

- Keep sensitive data out of the wrong hands by creating tough corporate policies and procedures.
- Encrypt data to make it difficult for outsiders to use if they do get their hands on it.
- Keep defenses strong by updating software with all security patches. Pay attention continually to security—not just annually when a software license fee comes due.

However, also recognize that human error is not always avoidable. When something goes wrong despite your best efforts, make sure the company is protected from liability with insurance that specifically addresses electronic data losses. NU

> "**Companies need to focus on data security** to avoid not only the cost of cleaning up security breaches but also the loss of reputation and trust that can affect future business growth."
>
> ***—Bob Ditmore***