DEALING WITH DATA LEAKAGE

Take steps to safeguard digital assets

Addresses, account numbers, Social Security numbers...are out there and could "leak" into cyberspace through something as innocent as employee error or as devious as intentional vandalism.

By Phil Zinkewicz

There's a relatively new phrase being used in IT circles these days: data leakage. It doesn't sound all that awful, does it? So, you've got a leak. Big deal! Management doesn't need to pay all that much attention to it. Someone will get around to it sooner or later.

However, as Tracey Vispoli, vice president of Chubb & Son and Global Cyber Solutions Manager for Chubb Specialty Insurance, puts it: "Leaks never look serious. You ignore a leaky faucet until you realize that you're losing 40 gallons of water a day. It's when you realize the impact of that leak that you start paying attention."

Vispoli describes data leakage as "the small bits and bytes leaving an organization day by day" and possibly getting into the wrong hands. "It could be personal information about employees, corporate trade secrets or even electronic keys to bank accounts. The information is leaking into the outside world, and its cost to business is difficult to quantify."

These days, a great many financial transactions take place without any face-to-face contact, and these transactions occur based on names and numbers—addresses, account numbers, Social Security numbers. People use their credit cards to make online purchases, or a bank's Web site to pay their bills. The numbers are out there and could "leak" into cyberspace through something as innocent as employee error or as devious as intentional vandalism.

In addition, more than 40 states have enacted legislation requiring companies to notify customers if their personal information may have been compromised. Even in states where notification is not required by law, failure to notify an individual of a potential identity breach may result in severe civil, regulatory and legal liability costs as well as potential damage to a company's reputation and loss of consumer confidence.

According to Forrester Research Senior Analyst Thomas Raschke, the cost of discovery and notification, which are typically required in every leak, is about $50 per lost record. For 20,000 lost records, this cost comes to $1 million. This is before any legal, public relations and lost customer costs.

According to Vispoli, some analysts put the cost per lost record at nearly $200, making the overall costs considerably higher.

Vispoli is responsible for designing and implementing new insurance and risk management products that respond to the changing vulnerabilities of Chubb's customers around the world. An expert in cybersecurity-related issues, Vispoli is a highly sought speaker and author on the topic, with recent bylined articles appearing in various trade publications.

"The problem is that data leakage is an unknown until the event is realized," she says. "You can't insure something that's unknown. A leakage could result in the ruining or damaging of someone's reputation. You can't insure that. But you can insure the monetary loss to an organization as the result of data leakage. And you can put plans into effect to prevent data leakage,"she says.

According to the Chubb executive, little has been done to put such plans into place. "It's a leap that management has not yet taken. Management must come to realize that data leakage is an everyday occurrence at companies, probably their very own. We have not gotten past the education stage yet. Management must come to realize that data leakage is not just an IT problem but also a problem of corporate economics.

"Once that message gets across, then plans need to be implemented to minimize the economic impact," Vispoli continues. "This is a heavy-