

Layoffs can make companies vulnerable to data theft

Experts say prevention can be as simple as checking e-mail logs

BY BETH FITZGERALD

WHEN A LAID-OFF employee walks out the door, critical company information may already be gone. The soon-to-be ex-worker may have e-mailed valuable data to a personal Web address — and intends to deliver that information to a company rival.

As the recession's depth and duration confounds forecasters, businesses are laying off experienced employees whose jobs gave them broad access to company intelligence: customer lists, financial information, maybe

More than severance pay

A whopping 59 percent of employees who lost or left their jobs last year admitted stealing company information, according to a survey released in February by the software company Symantec and IT research firm Ponemon Institute.

Among the survey findings:

- 53 percent downloaded company information onto a CD or DVD and 38 percent sent attachments to a personal e-mail account.
- 79 percent took data without an employer's permission.
- 82 percent said their employers did not perform an audit or review of documents before the respondent left his or her job.
- 24 percent of respondents had access to their employer's computer system or network after their departure from the company.

— Beth Fitzgerald

Asset Protection

even the engineering drawings for the company's next new gadget.

George Wade, director of computer forensics at the accounting and consulting firm **Sobel & Co.** in Livingston, said it is difficult, but not impossible, for companies to defend themselves against data leakage. Key steps include keeping a good inventory of essential data, knowing where it's stored and who has access to it, and staying alert for unusual data traffic.

"When you fire people, you don't just lose that person, you lose the information they take with them," said Wade, who before joining Sobel a year ago spent 20 years as regional security manager at **Lucent Technologies'** corporate security department in the Murray Hill section of New Providence.

Technology exists to safeguard data, but many companies can't afford to invest the money right now, Wade said. So he advises companies to start with the tools already at hand — and monitoring the flow of e-mail traffic is a key first step to defend the company data.

"Most companies have e-mail logs they can look at to see who is sending information, and where they're sending it," Wade said. "It can be as simple as looking at the frequency of messages, destination, the size of file attachments. An employee who normally only sent small text messages may suddenly start sending large attachments to a **Yahoo** or **Google** account."

Companies that outsource their e-mail



George Wade, director of computer forensics at Sobel & Co., says companies can take certain steps to protect against data theft, including noting the times of day large e-mail files were sent by employees.

management to a third party probably also have the ability to monitor e-mail logs, Wade said. Time of day may be a clue that something's up: an employee may transfer large data files late at night instead of during working hours when a data bulge would slow down the network and attract attention.

Wade said hackers who penetrate corporate computer firewalls and steal company secrets get most of the media's attention, "but the insider is a far greater problem." In his career, Wade said he's investigated multi-million-dollar intellectual property theft cases. And he's uncovered sabotage: fired workers who leave behind software weapons, known as "logic bombs" that dis-

able or delete company files.

Wade suggested that companies take steps to head off data theft by employees who fear they may lose their jobs during the recession:

- Take an inventory of critical data, where it is located and how well it is protected.
- Monitor access to the data and the activity on the e-mail system.
- Have a plan in place ahead of time if a data breach is suspected.

Once there are concerns that a data breach could happen, Wade said it may be necessary to bring in professionals and keep the perpetrator under surveillance for a while, to make sure the full extent of the breach is discovered. ♦

E-mail to bfitzgerald@njbiz.com



SOBEL & CO., LLC

Certified Public Accountants and Consultants
293 Eisenhower Parkway, Suite 290 Livingston, NJ 07039-1711