

Protecting Information from Insiders

Although organizations are making strides in protecting their sensitive information from outside threats, reports show they often are failing to protect it from the much greater threats posed by their own employees.

Nikki Swartz

In recent months, insider data theft stories have been grabbing headlines from tales of stolen laptops. Despite the growing risk, however, many businesses – even the biggest and most well known – are not properly protecting their sensitive information from inside threats.

For example, a federal jury recently convicted a former Coca-Cola secretary of conspiring to steal trade secrets from the world's biggest beverage maker in an effort to sell them to competitor Pepsi Co. Joya Williams faces up to 10 years in

prison, pending sentencing.

In February, *Computerworld.com* reported that a cell development technologist at Duracell Corp. admitted to stealing research related to the company's AA batteries. He e-mailed the information to his home computer and then forwarded it to two Duracell rivals.

In another case, a former DuPont scientist walked away with more than \$400 million worth of trade secrets after being hired by a rival company. Gary Min, who had worked at DuPont for 10 years, pleaded guilty in November to stealing proprietary

data from DuPont by illegally downloading or accessing thousands of documents stored in an electronic library. He faces a maximum of 10 years in prison and a fine of up to \$250,000.

Experts say too many firms are still relying on the old security model that advocated protecting information assets from the outside in through firewalls, intrusion detection systems, and other defenses. But those methods will not protect companies from insider threats.

“Frankly, we all have to actively stop thinking of insider vs. outsider”

and improve access controls for all users, Matt Kesner, chief technology officer at California law firm Fenwick & West LLP, told *Computerweek.com*. "It means looking at each and every person and machine as an island and deciding what rights and access each person and machine needs or doesn't need."

Paying closer attention to access rates would have provided DuPont a clear warning about the jeopardy of its intellectual property. According to court data, Min downloaded about 22,000 document abstracts from DuPont's Electronic Data Library server and accessed another 16,700 full-text PDF files. The documents related to DuPont's major products and technologies, including some that were in the research and development stage. Min illegally downloaded and accessed more than 15 times as many documents as the next-highest user of the DuPont database, according to *Computerworld.com*. Still, he wasn't caught until after he left the company.

Upon Min's resignation, an internal investigation exposed his activities, which DuPont then reported to the FBI and the U.S. Department of Commerce. Meanwhile, he was brazen enough to upload another 180 DuPont documents onto a laptop – owned by Victrex PLC, the England-based company he left DuPont to join – a full month after he had left DuPont. DuPont contacted Victrex officials, who seized Min's laptop and turned it over to the FBI.

Computerworld.com reported that a subsequent raid of Min's Ohio home in February 2006 uncovered several computers containing confidential DuPont information. Federal agents also found garbage bags filled with shredded DuPont documents, along with some remains of documents that had been burned in a fireplace. When agents entered the house, Min launched a software erasure program on one of the comput-

ers in an attempt to destroy the contents of its hard drive, according to the U.S. attorney's office.

Monitoring user access to mission-critical information and detecting unauthorized access to high-risk data are critical steps all companies should take to better protect their sensitive information.

Safeguarding Corporate Assets

The good news is that most companies are so frightened by the mere idea of intellectual property theft that a clear majority – 90 percent, according to a recent study by the Enterprise Strategy Group (ESG) – said they planned to implement new technologies to protect their sensitive data

during the following 12 months.

ESG's study, "Intellectual Property Rules," based on a survey of officials at organizations employing from 1,000 to more than 20,000 employees worldwide, revealed that:

- The biggest threat to companies' data is overwhelmingly internal, due either to malicious or negligent insiders or to faulty controls and oversight. While lost laptops and USB devices – and the data they contain – are a concern, such incidents actually represent only a small slice of the overall risk. Indeed, many organizations believe that intellectual property is likely to leak via e-mail or the Internet. But, ironically, ESG says there are still some organizations that do not inspect such obvious and well-documented leak points as web mail and instant messaging communications. (See sidebar on page 22.)
- E-mail is not always the most-likely source of confidential data breaches, however. One-third of companies' sensitive data and intellectual property exists in application databases where it can be centrally secured and managed. An additional 28 percent resides in file systems.
- The survey found that firms' most common forms of intellectual property, which require protection beyond personally identifiable information – such as credit card and Social Security numbers – range from financial information, contracts and agreements, source code, and competitive intelligence to design specifications, internal research data, trade secrets, and more.

The bottom line is that all organizations that want to protect their most valuable information assets must do better. The following recommendations, compiled from ESG

research and *Computerworld.com* reports, may not be cheap, fast, or easy, but security analysts suggest they are key to any effective corporate data protection strategy:

- *Automate intellectual property monitoring.* According to ESG, intellectual property assets are difficult to safeguard because they are dynamic; companies continually add to and evolve their intellectual property and other sensitive data while doing business. Thus, policies for protecting such assets must be continually reviewed and updated.

According to ESG's research, about 70 percent of organizations manually review their intellectual property policies on a quarterly or monthly basis. ESG said automating the detection of sensitive data in files, e-mails, databases, and shared servers is the first step toward reducing constant reviews of intellectual property protection policies. Manual reviews are expensive, time-consuming, and error-prone, ESG said, while automated discovery saves money, frees IT staff to perform other tasks, and is more accurate. An automated data-protection solution must address data at rest (resident in user directories or servers) and data in motion (as it traverses the network), ESG said. When all intellectual property can be automatically discovered, organizations can more effectively apply access policies.

- *Get control of the data.* Companies cannot control the sensitive data on their network if they don't know where that data is. Eric Ogren, ESG analyst, said an organization's sensitive data is spread throughout its corporate network, residing not just in databases, but also in e-mail messages, on individual computers, and in web

You've Got Mail – and Trade Secrets

Companies may have the most secure corporate e-mail system possible, but that means nothing when it comes to the very real risks to the organization when employees forward their office e-mail to free web-accessible accounts from such providers as Google, Yahoo!, and MSN.

Employees often forward their work e-mails – some of which may contain sensitive company information – to their personal accounts, bypassing any password requests meant to protect them.

No corporate breaches from this action have been reported to date, but experts urge organizations not to disregard the danger. They warn of corporate secrets leaking from the well-protected corporate network with a click of the "forward" button and fear forwarding e-mails might inadvertently expose proprietary information.

Corporate networks usually have several layers of protection against hackers, including special software and multiple passwords. Web-mail systems, however, have weaker security and could allow viruses or spyware to get through, meaning employees accessing these systems from the office could accidentally download bugs and infect the entire corporate network, according to a *New York Times* report.

Another risk, the *Times* noted, is that employees' use of outside e-mail may result in companies being unable to comply with federal rules requiring them to archive corporate e-mail, which is discoverable in the event of a lawsuit, because messages sent from outside e-mail accounts do not pass through the corporate network.

Along those lines, many technology professionals worry that Google and other web-mail providers may actually own the intellectual property in the e-mail that resides on their systems, according to the *Times*. Gmail's terms of service, however, state that e-mail belongs to the user, not to Google, and the *Times* reported that the company's extensive privacy policy ensures no humans at Google read user e-mail.

In an attempt to fully protect themselves, though, some companies have gone so far as to ban employees from accessing outside e-mail in the workplace. And, according to e-mail security firm Proofpoint, 37 percent of U.S. firms surveyed said they monitor employees' use of web mail.

portals. This information comes in many forms and can be found in many types of documents and files. Rather than implementing one set of controls for all data types, he suggests categorizing the data and choosing the most appropriate set of controls for each data class. Tools are available that can automatically scan company networks and identify sensitive data where it resides. Many of these can be used to separate data into different categories based on a company's policies.

- **Monitor content.** As companies web-enable their business and link up with networks owned by partners, suppliers, and customers, they still must keep track of what is flowing over their networks as well as monitor network traffic, according to *Computerworld.com*. There are products that can help companies inspect e-mail, instant messages, P2P file-sharing systems, web postings, and FTP sites for data that may be escaping a firm's network. These tools sit near network gateways and issue alerts when they find suspicious data packets. Many can also block data or encrypt it when it exits the network.
- **Watch the database.** A company's information assets can be found in its databases, so it is critical to know not only who is accessing them, but also when, where, how, and why. *Computerworld.com* suggests employing database activity monitoring tools for this purpose. Such tools also monitor what users and administrators are doing with their access privileges and either prevent certain actions – such as modifying, copying, deleting, or downloading large sets of files – or send out alerts when they are attempted. They also can provide clear audit trails that track when people try

to override corporate policy. Encrypting sensitive data in databases is another must-do for all companies who haven't done so, *Computerworld.com* said.

- **Limit access.** Many companies give employees far too much access, experts say. The goal should be to give insiders as much access as they need to do their jobs, but no more. Monitoring user access to mission-critical information and detecting unauthorized access to high-risk data are critical steps all companies should take to better protect their sensitive information. Access policies should also include controls that send out alerts when an employee who usually accesses a certain number of documents a day suddenly starts accessing a much larger number.

- **Cover endpoints.** Small, portable devices – memory sticks, PDAs, and iPods – make it easy for employees to walk out the door with large volumes of corporate data. While most employees innocently employ these devices to work from home, the practice is still risky. Companies must implement policies and technology to centrally control and monitor what devices can be attached to corporate networks and what data can be downloaded, uploaded, and stored on them.

Of course, employing such methods cannot guarantee that an organization will not experience an insider breach. But gaining better control over valuable information, no matter where it resides, is always a smart move. ■

Nikki Swartz is a freelance writer based in Kansas City, Missouri, and former Associate Editor of The Information Management Journal. She may be contacted at nikkiswartz@hotmail.com.

References

"Intellectual Property Breaches Plague 32 Percent of Surveyed Companies." Available at www.sys-con.com/read/344626.htm (accessed 16 March 2007).

Jaques, Robert. "Intellectual Property Theft Spreading Fast." *ITNews.com*, 6 March 2007. Available at www.itnews.com.au/print.aspx?CIID=74707&SIID=35 (accessed 7 March 2007).

"Lessons from the DuPont Breach: Five Ways to Stop Data Leaks." *Computerworld.com*, 28 February 2007. Available at <http://computerworld.com/action/article.do?command=viewArticleBasic&articleId=9011976&pageNumber=1> (accessed 19 March 2007).

Stone, Brad. "Firms Fret as Office E-Mail Jumps Security Walls." *The New York Times*, 11 January 2007. Available at www.nytimes.com/2007/01/11/technology/11email.html?_r=1&th&emc=th&oref=slogin (accessed 19 March 2007).

Vijayan, Jaikumar. "DuPont Data Theft Shows Insider Risks." *Computerworld.com*, 19 February 2007. Available at http://computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=security&articleId=283564&taxonomyId=17&intsrc=kc_top (accessed 6 March 2007).

Read More About It

To access the Enterprise Strategy Group's "Intellectual Property Rules," visit www.reconnex.net/docs/Reconnex_ESG_Brief_Feb07.pdf.