REAL WORLD CASE 4

Raymond James Financial, BCD Travel, Houston Texans, and Others: Worrying about What Goes Out, Not What Comes In

It's not what's coming into the corporate network that concerns Gene Fredriksen; it's what's going out. For the chief security officer at securities brokerage Raymond James Financial Inc. in St. Petersburg, Florida, leakage of sensitive customer data or proprietary information is the new priority. The problem isn't just content within e-mail messages, but the explosion of alternative communication mechanisms that employees are using, including instant messaging, blogs, FTP transfers, Web mail, and message boards. It's not enough to just monitor e-mail, Fredriksen says. "We have to evolve and change at the same pace as the business," he explains. "Things are coming much faster."

So Fredriksen is rolling out a network-based outbound content monitoring and control system. The software, from San Francisco–based Vontu Inc., sits on the network and monitors traffic in much the same way that a network-based intrusion-detection system would. Rather than focusing on inbound traffic, however, Vontu monitors the network activity that originates from Raymond James's 16,000 users. It examines the contents of each network packet in real time and issues alerts when policy violations are found.

Network-based systems do more than just rule-based scanning for Social Security numbers and other easily identifiable content. They typically analyze sensitive documents and content types and generate a unique fingerprint for each. Administrators then establish policies that relate to that content, and the system uses linguistic analysis to identify sensitive data and enforce those policies as information moves across the corporate LAN. The systems can detect both complete documents and "derivative documents," such as an IM exchange in which a user has pasted a document fragment.

When BCD Travel began to investigate what it would take to get Payment Card Industry (PCI) certification for handling customer credit card data, Brian Flynn, senior vice president of technology, realized that he didn't really know how his employees were handling such information. Not only could PCI certification be denied, but the travel agency's reputation and business could also be harmed. At the National Football League's Houston Texans, IT Director Nick Ignatiev came to the same realization as he investigated PCI certification.

In both cases, vendors they'd been working with suggested a new technology: outbound content management tools that look for proprietary information that might be leaving the company via e-mail, instant messaging, or other avenues. Flynn started to use Reconnex's iGuard network appliance, with vivid results. "It was a shock to see what was going out, and that gave us the insight to take action," he says. After Ignatiev examined his message flow using Palisade Systems's PacketSure appliance, he too realized that his employees needed to do a better job protecting critical data, including customer credit cards, scouting reports, and team rosters.

How does the technology work? Basically, the tools filter outgoing communication across a variety of channels, such as e-mail and IM, to identify sensitive information. They're based on some of the same technologies—like pattern matching and contextual text search—that help antivirus and antispam tools block incoming threats.

Tools typically come with basic patterns already defined for personally identifiable information, such as Social Security and credit card numbers, as well as templates for commonly private information, such as legal filings, personnel data, and product testing results.

Companies typically look for three types of information using these tools, notes Paul Kocher, president of the Cryptography Research consultancy. The first, and easiest, type is personally identifiable information, such as Social Security numbers and credit card information. The second type is confidential company information, such as product specifications, payroll information, legal files, or supplier contracts. Although this information is harder to identify, most tools can uncover patterns of language and presentation when given enough samples, Kocher notes. The third category is inappropriate use of company resources, such as potentially offensive communications involving race.

The traditional security methods may restrict sensitive data to legitimate users, but Flynn and Ignatiev found that even legitimate users were putting the data, and their companies, at risk. At BCD Travel, a corporate travel service, nearly 80 percent of its 10,000 employees work in call centers and thus have legitimate access to sensitive customer information. BCD and the Texans did not find malicious activity; instead, they found people who were unaware of security risks, such as sending a customer's credit card number by e-mail to book a flight or room from a vendor that didn't have an online reservations system.

Fidelity Bancshares Inc. in West Palm Beach, Florida, is using the message-blocking feature in PortAuthority from PortAuthority Technologies Inc. in Palo Alto, California. Outbound e-mail messages that contain Social Security numbers, account numbers, loan numbers, or other personal financial data are intercepted and returned to the user, along with instructions on how to send the e-mail securely.

Joe Cormier, vice president of network services, says he also uses PortAuthority to catch careless replies. Customers often send in questions and include their account information. "The customer service rep would reply back without modifying the e-mail," he says.

"The challenge with any system like this is they're only as valuable as the mitigation procedures you have on the back end," notes Fredriksen. Another key to success is educating users about monitoring to avoid "Big Brother" implications. "We are making sure that the users understand why we implement systems like this and what they're being used for, he says.