

Counting On Data Loss Prevention

Financial Firms Use DLP to Protect Customer Data and Their Own Reputations

There's a treasured family heirloom in my home office: a box of letters my father wrote during the Second World War. With his careful penmanship, Dad described the exploits of his bomber crew; with equal care, a military censor combed through those letters before they left England, literally slicing out words that might betray strategic information should the mail fall into enemy hands.

In a sense, that censor's razor blade was an early form of Data Loss Prevention (DLP). The goal of DLP is to stop valuable digital information from leaving an organization, whether intentionally or inadvertently. Larry Ponemon, chairman and founder of the Ponemon Institute, a think tank dedicated to privacy and data protection, describes DLP this way: "Like a firewall prevents bad guys from getting in, DLP prevents the negligent employee or insider from leaking information out."

DLP can have several components, including data discovery, content monitoring and filtering, encryption, and identity management. (See "Data Loss Prevention Glossary" sidebar on page 19.) The market's evolving, so not all vendors agree on the terms and their meanings. "I cover probably 30 different DLP vendors, and I would say half of them use different terminology," says Brian E. Burke, program director for security products at analyst firm IDC. "There's a lot of confusion out there."

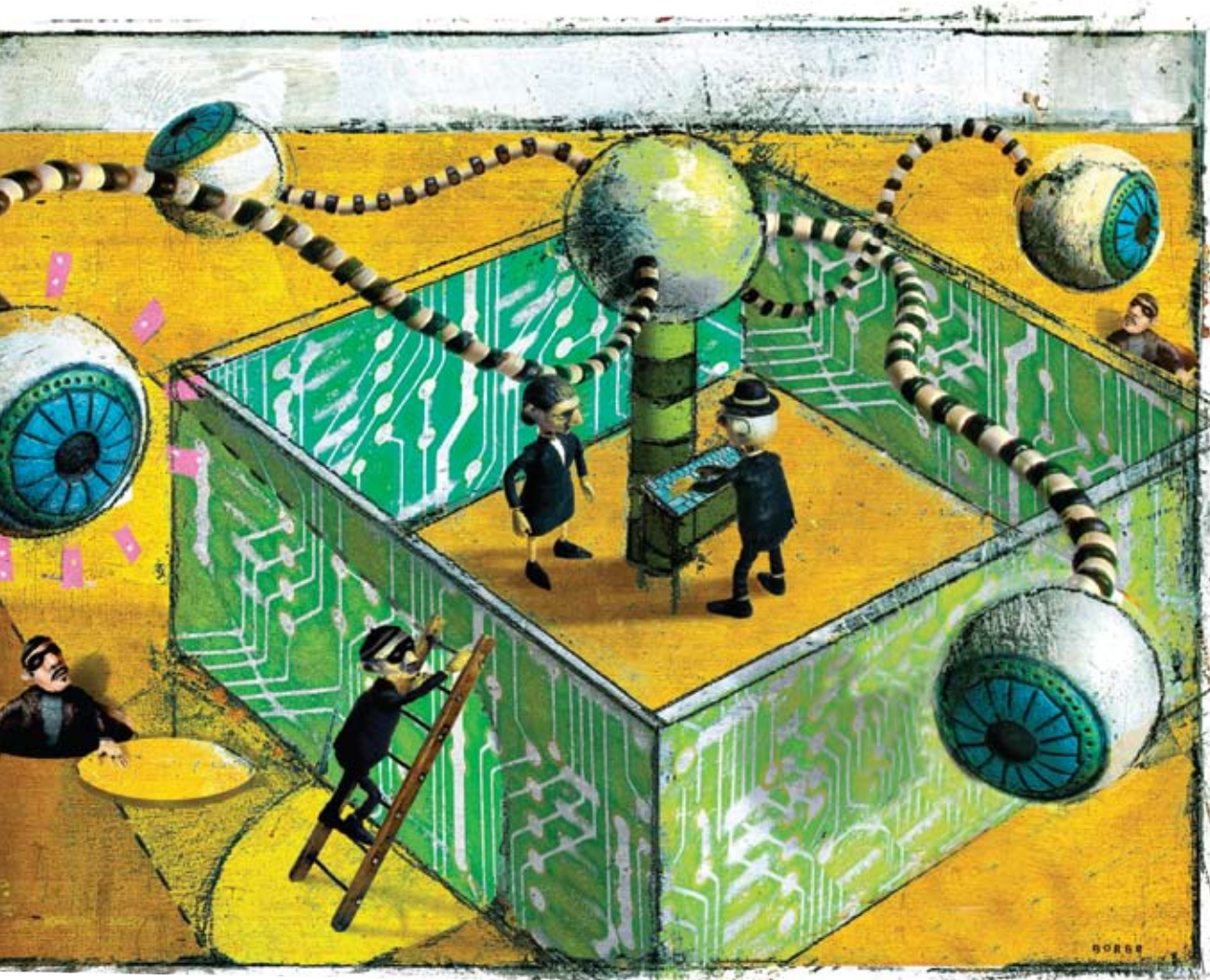
Many drivers

Though DLP's roots can be traced to the early days of computing, its existence as a distinct category in information security is fairly new. One thing's for sure: the

category's booming. "If you attended the RSA conference this year, you would have seen signs on probably 50 percent of the booths indicating they do DLP," says Craig Shumard, chief information security officer at CIGNA, a provider of health insurance and related benefits.

Financial services firms operating in the United States—a sector that includes insurers such as CIGNA—have been early adopters of DLP technologies for several reasons. They operate in a highly regulated environment, answering to the Gramm-Leach-Bliley Act (GLBA), Sarbanes-Oxley (SOX), Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry Data Security Standard (PCI DSS) requirements, and more than 40 different state laws dictating data privacy standards. (The regulations requiring institutions to notify customers of data breaches are typically state laws, though federal banking agencies also maintain guidelines regarding customer notification.) Financial institutions are keenly aware that their customers are protective of their personal data and are prone to change providers if they don't feel properly protected.

By Fred Sandmark



This higher expectation of protection means more is at risk: according to Ponemon, a data breach at a financial services organization costs \$239 per compromised record, or more than 21 percent higher than the average.¹

Donna Durkin, the information security officer for Computershare, North America, a global services and technology provider for the securities industry that serves 14,000 corporations and 100 million shareholder and employee accounts, indicates several factors led her company to adopt DLP—including the negative media exposure its competitors received in the wake of data breaches, regulatory requirements, and the need to demonstrate rigorous data protection standards to Computershare’s clients. “It’s a combination of those three things,” she says. “We want to stay in the

forefront—not only when new technologies emerge that help us address things like protection of privacy information, but in general, from a marketing and competitive perspective.”

The reputation and competitive aspects can’t be downplayed, according to Burke. “Often that’s much more costly than any government or industry fine,” he says. The market bears this out, Ponemon says; his research shows that retail banks are the number one purchasers of DLP solutions, even though he has found no direct correlation between data breaches and identity theft.²

Other factors are at work, too. “Financial institutions are among the biggest data hoarders out there. A large institution can have petabytes worth of data,” says George Tubin, senior research director at

TowerGroup, a financial industry advisory firm. And the data tends to get spread around the company, as analysts and marketers duplicate and massage it. With the workforce becoming more mobile, and the proliferation of sensitive data resting on thumb drives, laptops, PDAs, iPods, and other personal devices, understanding where confidential data lives, where it’s going, and who is accessing it becomes more complex and difficult to control. “Historically, banks haven’t kept good track of where sensitive data was going in the institution,” Tubin says. As banks look to provide customers with a seamless experience across a growing number of channels, including online and mobile banking, maintaining high levels of service and agility presents new complexities and challenges for keeping customer data safe.



Craig Shumard,
Chief Information
Security Officer, CIGNA

And being number crunchers by profession, financial firms also know that protecting against data loss can be a good investment. Ponemon has found that data breaches tend to scare customers away from online banking, which typically is a bank's most profitable channel and currently outpaces the number of transactions in all other channels, with no sign of slowing down.

Correcting behavior

Wise firms aren't using DLP simply to improve their defensive posture; they're using it as a tool to correct employee behavior. One example of how this works: Symantec Data Loss

Prevention Network Monitor and Symantec Data Loss Prevention Network Prevent not only can block an outgoing email containing confidential data, but they can also pop a message onto the sender's desk informing him or her of the action. At Computershare, Durkin says that notifying users of potential leaks has altered their behavior for the better. "That's been the most noticeable change," she says. "As time goes on, the number of incidents [of employees attempting to send confidential data] goes down on its own, substantially. It's a clear indication that employees are more conscious of what they're doing."

Because incidents of policy violations are also reported to Computershare's Symantec Data Loss Prevention Enforce Platform, Durkin and her team use the information to identify users who need special assistance or training. In this way, the DLP system becomes another tool for Computershare to increase the level of security awareness across the organization.

To ensure that DLP doesn't slow day-to-day operations, Computershare's IT team set an internal service level: to respond to DLP-related alerts in 15 minutes or less. This, too, has improved employee behavior and reduced opportunities for employees to circumvent the DLP solution. "Getting immediate feedback to the end user has

resulted in fewer incidents over time," Durkin says.

Improving operations

Both Computershare and CIGNA indicate that their DLP implementations have uncovered ways they can improve their operations—a fact that also expands DLP's value beyond defense.

Research shows that most data loss is inadvertent, not malicious; IDC estimates that 80 percent of such incidents are accidental.³ Still, the number of emails initially blocked by Symantec Data Loss Prevention after its October 2007 deployment at Computershare indicated that certain employees had a genuine business need to transfer sensitive files; they simply lacked a secure channel. "We sat down with individual business groups and analyzed what types of information they were trying to get to clients, and in what format," Durkin says. "It prompted us to implement a better secure file transfer option for client-facing staff; since we started the [Symantec] implementation, we've set up nearly 1,500 new secure file transfer accounts with clients."

At CIGNA, Shumard says that the breadth of its Symantec Data Loss Prevention solution—compared with the email monitoring point solution the company formerly employed—has streamlined information security operations. "We've seen tremendous gains in efficiency by the features and functionality of the tool that we have now, because of the ability to handle a lot of different platforms and protocols," he says. (See "The Symantec Data Loss Prevention Risk Assessment" sidebar below.)

DLP can also help improve efficiency related to data at rest. As part of DLP implementations, Tubin recommends that clients perform thorough data discovery on their systems. This identifies files that need to be protected. "We can't protect something if we don't know that it actually exists," he explains. The process of discovering unsecured files containing confidential information also locates orphaned

The Symantec Data Loss Prevention Risk Assessment

Customers that evaluate Symantec Data Loss Prevention are given a complementary 48-hour risk assessment to help them quantify and qualify their risk of data loss. The assessment shows how much confidential and sensitive data is on the network, where it is stored, what data is leaving the network, how that data is being transmitted (email, removable media, etc.), what regulations are being violated, and more.

Donna Durkin's group at Computershare North America went through the risk assessment in the fall of 2007. Durkin

says she wasn't surprised by the results. "We knew we had data stored in various places that contained privacy information," she says. "We knew approximately what the counts were going to be, and what we were going to find," in part because the company had experimented with some open-source and internally developed tools. "The ease of use and the implementation of the product were probably the most surprising," she says; Computershare had set aside a week for the project, but data discovery began within an hour on the first

day. She was also impressed with the accuracy of the predefined policies for financial services organizations.

At CIGNA, Craig Shumard also was not surprised by the results of the risk assessment performed in early 2007. "The results, quite frankly, came out pretty much what I expected," he says. "We had a pretty good handle on our needs going into the assessment. What we were looking for was help in meeting those needs." In particular, Shumard found it "compelling" to see data in motion and data at rest on a single dashboard.

data (extant in many financial companies due to mergers and acquisitions) and redundant data that can be deleted.

Looking ahead

As DLP becomes a standard part of financial services security—Shumard calls it “one of the fundamental building blocks of an overall information security program,” alongside antivirus, antispam, and perimeter protection—it’s also finding a home in other industries. Indeed, Burke says that a DLP-related concern, “employees inadvertently exposing confidential information,” is now seen as the number one threat to enterprise security among all companies IDC surveys.⁴ (See “Importance of Top 10 Threats to Enterprise Security” on page 19.)

“Any business with trade secrets, customer lists, marketing plans, or other proprietary information should look at DLP,” Burke says. “We’ve talked to a company that makes wallboard about DLP. They’re very concerned about their intellectual property, how they put their product together, design schemes and research plans, things of that nature.”

But things of that nature present a DLP challenge. “It’s easy to identify a social security number, and only a little more difficult to identify account numbers,” Burke says. “But that’s what’s called structured data. When you start looking at unstructured data, it becomes much more difficult. You need a really sophisticated analysis engine to understand if something like that is a violation of policy.”

Ponemon agrees. “The better a DLP works on unstructured or messy data, the more valuable and effective it’s going to be,” he says. Companies wanting to use DLP to protect this sort of data should press vendors to demonstrate their solutions’ abilities.

New communication channels are another DLP hurdle. Shumard sees this today at CIGNA, citing webmail and peer-to-peer networks. “The challenges associated with DLP continue to evolve,” he says. “While most organizations like ours make every attempt to block those behaviors and tools, avenues continually evolve for circumventing those obstacles. So the robustness of the DLP tool, and the ability to handle new challenges, is something that we continually look at.”

This evolution of communication spans industries. “We actually see this at IDC,” Burke says. “New employees don’t use email; that’s not how they communicate. They chat, they use IM, they use social networking sites, they use the web. And they’re bringing those tendencies to the workplace. The web is definitely the next hot area of DLP.”

It’s hot because what’s changing is not only technology; it’s attitudes toward work, data, and self. On the one hand, individuals are increasingly protective of personal information; on the other hand, employees who handle

data make fewer distinctions between their personal and professional lives. “When you think about how social networking and virtual worlds have evolved, and you think about the way people work from home or the train or the office, there’s a lot of blurring of what’s company versus personal,” Shumard says. “That’s a significant challenge.” And this is a challenge that automated DLP solutions hope to meet, because it won’t be solved by a person reading letters and wielding a razor blade. ■

Fred Sandsmark is a regular contributor to CIO Digest. His father, Hardy, flew 42 missions during World War II.

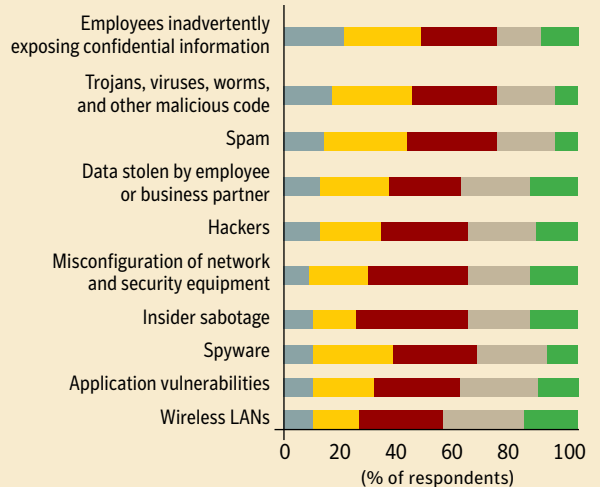
¹ “2007 Annual Study: U.S. Cost of a Data Breach: Understanding Financial Impact, Customer Turnover, and Preventative Solutions,” Ponemon Institute, November 2007.

² This data is based on general research conducted by the Ponemon Institute, Inc.

³ IDC indicates that this data point is widely accepted as an industry norm.

⁴ Brian E. Burke, “Information Protection and Control Survey: Data Loss Prevention and Encryption Trends,” IDC, May 2008.

Importance of Top 10 Threats to Enterprise Security



Significant Threat ■ 5 ■ 4 ■ 3 ■ 2 ■ 1 No Threat

Source: “Information Protection and Control Survey,” IDC, 2007

Data Loss Prevention Glossary

Content Monitoring and Filtering (CMF):

Constant, ongoing checking of the data that is in use on a computer; screening out data that does not conform to security policies.

Data at Rest: Data that resides on disks, whether on a server in a data center or on individual computers, including portable computers.

Data Discovery: An automated process of checking every endpoint on a network for confidential or unsecured data.

Data in Motion: Data that’s traveling on a network, such as email or IM traffic.

Encryption: Translating data into a form that can only be read by a person or system with the appropriate digital “key.”

Identity Management: The process of identifying an individual using a computer system and assigning that individual rights and privileges based on that identity.

Personally identifiable information: Any piece of data that can be linked to a single individual.

Policy: A written document that spells out how an organization deals with security matters; “policy” is also used to describe the rules by which DLP systems grant permissions to users.

Structured Data: Data residing in fixed fields, such as a database. Sometimes “structured data” denotes any data that has a rigid format, such as a Social Security number.

Unstructured Data: Data that does not conform to a fixed field or format, such as PDF or word processing documents.