



A n a l y t i c s R e p o r t

Risk Intolerant: Defense in Depth And the Rise of Data Loss Prevention

Security pros continue to move from protecting systems to protecting data, and it's about time. Attackers are getting smarter, and complex new applications make repelling them ever harder. Technologies like data loss prevention, or DLP, purport to help. Here's what you need to know about this emerging discipline.

By Randy George



A n a l y t i c s R e p o r t

T A B L E
O F
C O N T E N T S

5	Author's Bio
6	Executive Summary
8	Research Synopsis
9	A Holistic Approach to DLP
10	Impact Assessment
19	The Genesis of Network DLP
21	Big Brother Is Watching
24	Regulatory Compliance Is Driving This Train
27	ROI Analysis: Data Loss Prevention
28	Strategy for DLP Success From Network to Endpoint
36	Appendix



A n a l y t i c s R e p o r t

T
A
B
L
E

O
F

C
O
N
T
E
N
T
S

- 9 Figure 1: Existing Data Protection Capabilities
- 11 Figure 2: A Comprehensive Data Loss Prevention Infrastructure
- 12 Figure 3: Sources of Data Loss
- 13 Figure 4: Identity Authentication
- 14 Figure 5: Changing Passwords
- 15 Figure 6: Disk Encryption on Mobile Devices
- 17 Figure 7: Prevent, Protect and Prove
- 18 Figure 8: Data Encryption on Removable Media
- 19 Figure 9: Greatest Risk for Data Loss
- 20 Figure 10: Information Loss Concerns
- 21 Figure 11: Corporate Use of IM
- 22 Figure 12: Personal E-mail Access
- 23 Figure 13: DLP Product Capabilities
- 24 Figure 14: Factors Driving Interest in DLP
- 25 Figure 15: Impact of Compliance on DLP Decision
- 26 Figure 16: Satisfying Regulations With DLP
- 28 Figure 17: Four-Step Framework for Stopping Data Loss
- 29 Figure 18: 10 Endpoint Leakage Avenues You Must Block
- 30 Figure 19: 3 Endpoint Leakage Scenarios You Must Account For
- 31 Figure 20: 5 Key Network DLP Capabilities
- 32 Figure 21: Key Data Protection Controls
- 33 Figure 22: Desired DLP Features



A n a l y t i c s R e p o r t

T A B L E O F
CONTENTS

34	Figure 23: DLP Concerns
36	Figure 24: Job Title
37	Figure 25: Will DLP Be A Security Standard?
37	Figure 26: PII Storage Policies
38	Figure 27: Technology to Enforce PII Storage Ban?
39	Figure 28: Company Revenue
40	Figure 29: Use of Data Loss Prevention
40	Figure 30: Company Size
41	Figure 31: Industry



A n a l y t i c s R e p o r t

Randy George
InformationWeek
Analytics



Randy George has covered a wide range of network infrastructure and information security topics in his three years as an *InformationWeek* and *Network Computing* contributor and security beat owner. He has 13 years of experience in enterprise IT as a senior-level systems analyst and network engineer and holds professional certifications from Microsoft, Cisco and Check Point.

Randy earned a BS in computer engineering from Wentworth Institute of Technology and an MBA from the University of Massachusetts Isenberg School of Management.



A n a l y t i c s R e p o r t

Executive Summary

Between Web 2.0 apps, instant messaging, file sharing, smartphones, Facebook, Twitter and other as-yet-to-be-invented communication channels, employees have ample opportunity to lose data. Security professionals understand this and realize that a paradigm shift is under way, from endpoint and network protection toward safeguarding information. The adjustment is logical and necessary, because the crown jewels of your organization aren't notebooks and smartphones, but the digital business assets stored on them.

The trick is balancing wants and needs.

Knowledge workers want access to their data at any time, on the platform of their choice, using their preferred sets of tools and applications. The CEO wants controls to make sure your organization won't be the next data loss poster child, without adversely impacting productivity.

The CIO wants some aspirin, because it's shaping up to be another trying budget season.

With so many avenues open to outside attackers and insider threats, and with so many operating system and browser deficiencies being exploited by ever-more-clever malware developers, IT *needs* to accept that it's almost impossible to prevent data leakage by concentrating defenses on desktops, servers and the network perimeter. The term "defense in depth" is taking on additional intensity.

A concern about emerging data loss prevention (DLP) technologies cited by many security professionals we've spoken with is employee resistance



A n a l y t i c s R e p o r t

Executive Summary

to IT scanning their communications, because of both privacy and performance concerns. This is summed up by one poll respondent.

“The Achilles heel of DLP is that the people with access to the most sensitive data are also the people who are powerful enough to exempt themselves from enforcement tools and policies,” says an IT manager at an engineering and development services firm. “Senior managers and sales staff often will not allow policy to interfere with their personal convenience and often give short shrift to advice and education about data security. So even in organizations with strict policies, the overall risk is often not reduced sufficiently to justify the expense of DLP or the inconvenience to production employees.”

In this *InformationWeek* Analytics report, we’ll investigate the macro-level dynamics that are driving comprehensive DLP initiatives worldwide and discuss some ancillary tools and technologies that will help solve data leakage problems. But a discussion of market trends does nothing for IT groups that need a strategy, now. For them, we’ll map out a battle plan complete with tools, technologies and best practices that can keep your information assets from slipping through your fingers and into the hands of professional data thieves the world over.



A n a l y t i c s R e p o r t

Research Synopsis

Survey Name: *InformationWeek* Analytics Data Loss Prevention Survey

Survey Date: March 2009

Region: North America

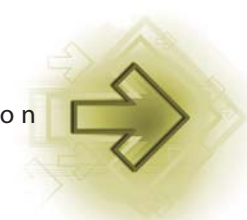
Number of Respondents: 218

Purpose:

To determine the role of data loss prevention technologies in enterprise security strategies.

Methodology:

InformationWeek Analytics surveyed business technology decision-makers at North American companies. The survey was conducted online, and respondents were recruited via an e-mail invitation containing an embedded link to the survey. The e-mail invitation was sent to qualified *InformationWeek* subscribers.



Analytics Report

A Holistic Approach to DLP

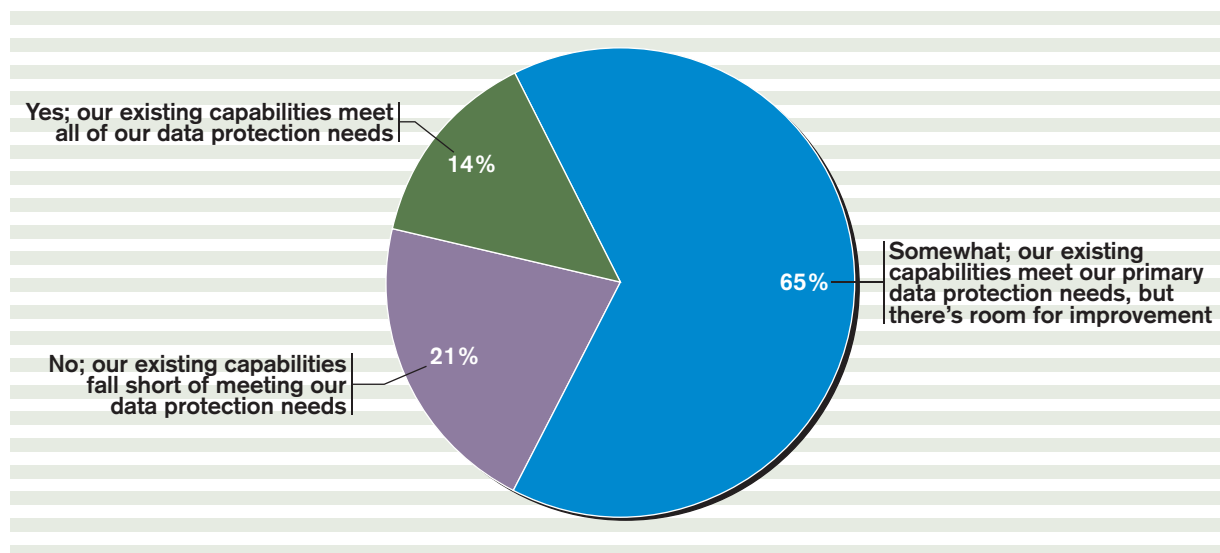
Ask 200-plus business technology professionals about data loss prevention, as *InformationWeek Analytics* did for this report, and you'll get a number of perspectives. This technology is still new enough that implementation war stories are rare. What's not so scarce, unfortunately, are cautionary tales of why you need DLP in the first place. One that first surfaced in the *San Jose Mercury News* concerns Abdirahman Ismail Abdi, an employee of the California Water Services Company who resigned from his job April 27. That night, Abdi was spotted in the CWSC facility, allegedly wiring \$9 million in company funds to an offshore account in Qatar. That Abdi was in a position to pull off a heist of that magnitude after his resignation drives home the message that DLP is about more than just protecting an Excel spreadsheet that contains your employees' personal information. It's about placing a vault around all critical systems, digital assets, intellectual property, personally identifiable information (PII) and especially financial data. It also argues for identity management and swift deprovisioning.

As we're learning in our *InformationWeek* Rolling Review of DLP systems (four tested, two to

Figure 1

Existing Data Protection Capabilities

Do you feel that your existing capabilities to protect corporate data, including reporting, threat response, and alerting on policy violations, are adequate?



Data: *InformationWeek Analytics* Data Loss Prevention Survey of 218 business technology professionals



Analytics Report

go), vendors assert that a robust and comprehensive data loss prevention strategy centers largely on filtering technology, endpoint protection and data encryption. But as *InformationWeek* contributor Joe Hernick discusses in our recent endpoint security Analytics report, that's just the beginning. Successful DLP programs have a few common traits: They cut across a wide range of disciplines. They enjoy support from the very top of the organization. And they employ not just technology but firm usage policies and procedures that are enforceable, understandable and accepted by all parties.

While the focus of this Analytics report is on the growth, capabilities, compliance requirements and key drivers for a successful network DLP deployment, a multi-tiered approach to protect-

Impact Assessment: Data Loss Prevention Suites

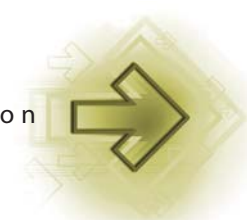
	● Benefit	● Risk
IT Organization	○ ● ● ● ● Enterprise DLP gives IT new capabilities for discovering and preventing loss of critical data. It's cheap to replace a laptop, but notification is expensive. Focusing your security strategy on content protection makes your organization a more difficult target to attack. DLP also aids in data discovery efforts.	○ ○ ● ● ● Complex, heterogeneous environments that are subject to aggressive compliance requirements will need to allocate significant resources to ensure the DLP software works properly while maintaining business agility.
Business Organization	○ ○ ● ● ● If an investment in DLP prevents a data breach that requires notification (read: bad publicity), the benefits are incalculable. For small shops with no compliance requirements, cost may outweigh the benefit now, but keep an eye on this technology; prices will inevitably drop.	○ ● ● ● ● A poorly executed DLP implementation could put a damper on productivity. Without high-level backing and education, a full implementation that includes keyword monitoring inside e-mail and instant messages might be met with resistance from employees on privacy grounds.
Business Competitiveness	○ ○ ● ● ● If you can use DLP effectively to mitigate information leaks, quash corporate espionage, and quickly prove compliance and security standards to management and auditors, you will have an advantage over many of your competitors.	○ ○ ○ ○ ● An investment in DLP is an intangible, an insurance policy. While DLP won't directly drive you ahead of the competition, you might feel that way if a competitor crashes and burns from a TJX-like data breach.



Bottom Line

In a tough economy, attackers want your data for profit, and layoffs increase the insider threat level. Applications are getting more complex—without getting any more secure. Infosec pros need to boogie further down the evolutionary path that began with a hard perimeter defense and moved to defense in depth. Both are still important, of course, but we need to add data-centric protections, including new DLP suites where budgets allow.

Note: Number of dots indicates level of benefit and risk; one dot equals low benefit/risk, five dots equal high benefit/risk.



Analytics Report

ing key data and systems ties together the big-picture technologies pictured in Figure 2, below.

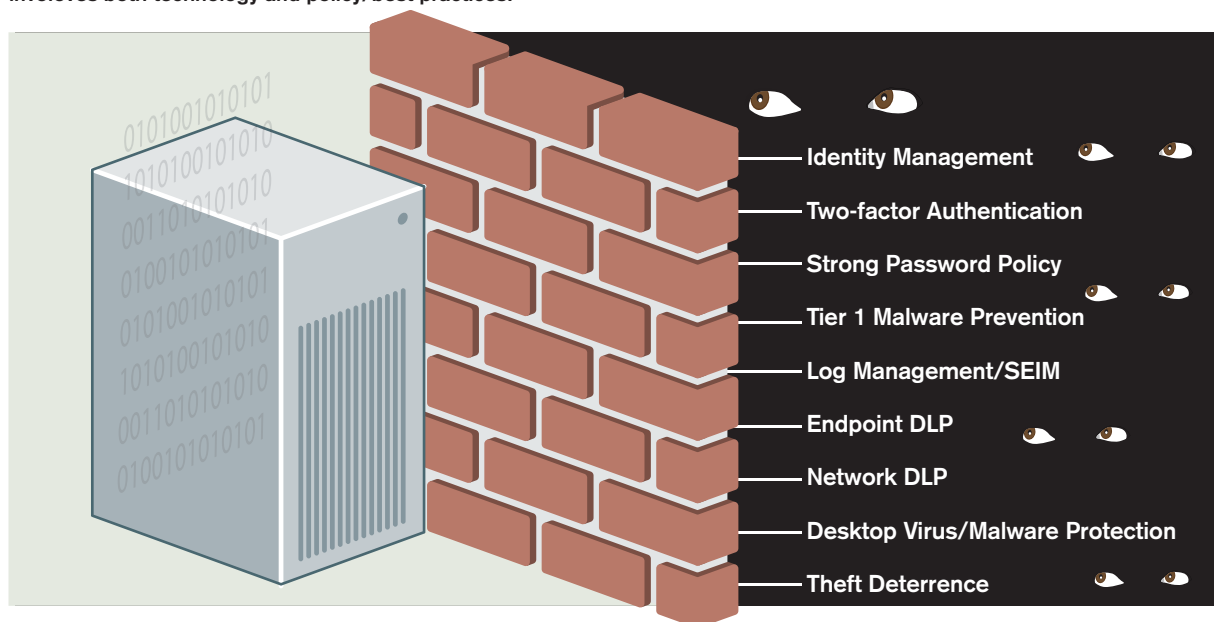
Since we began our DLP Rolling Review, we've heard from many organizations that are scrambling to implement some sort of initiative quickly to comply with an increasingly complex and stringent regulatory environment. But our advice is to first step back and catalog all core points of vulnerability. In the *InformationWeek* security lab, we've coined a security strategy for doing this evaluation that we trust is not trademarked elsewhere: "Prevent, Protect and Prove." In other words, *prevent* spyware with a malware filter, *protect* your data with a DLP suite and other tools, and be able to *prove* to auditors that you can forensically detect attacks with enterprise log management and network behavioral analysis systems.

When building a complex security infrastructure, especially one that cuts across many different product types, it often helps to frame each technology genre in terms of the real-world problems it solves. We'll cover DLP in depth, but let's first touch on a few additional technologies that will complement your implementation.

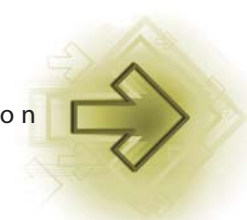
Figure 2

A Comprehensive Data Loss Prevention Infrastructure

Building a strong protective infrastructure requires defence in depth, from the desktop to network-based controls, and involves both technology and policy/best practices.



Data: InformationWeek Analytics



Analytics Report

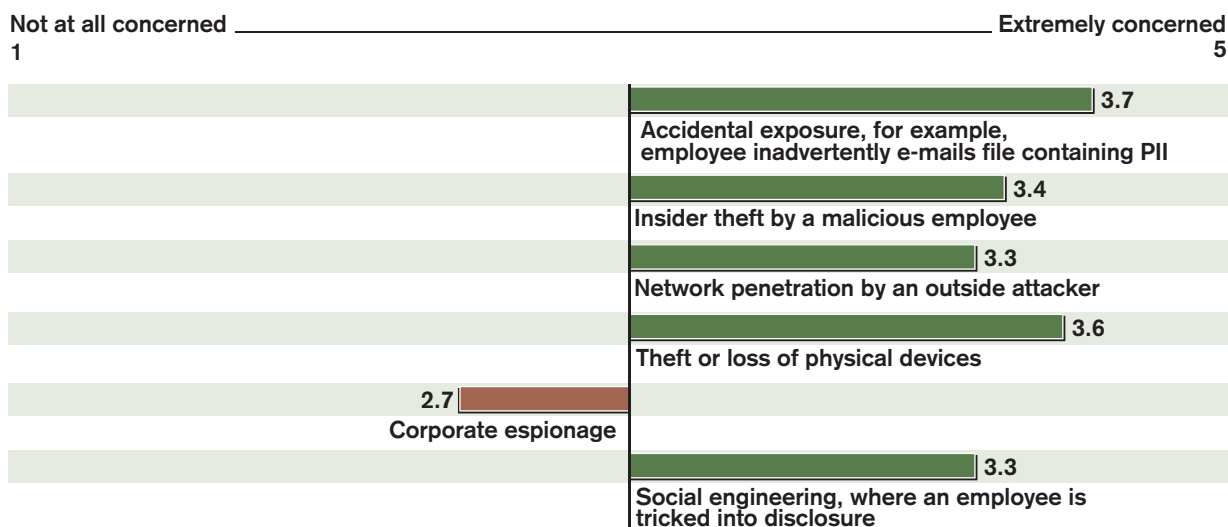
Identity management's role in preventing data loss: Poor account management isn't just a problem in large enterprises. Even small and midsize shops can have an unacceptably large number of IT and even line-of-business personnel with administrative access to your domain and its data. Administrative access sprawl is a huge security risk for any organization, but it's even worse in the absence of infrastructure and policies to disable network access for employees who resign or are let go. While California Water Services officials have not made public Adbi's exact position, several theories regarding the recent break-in suggest that his network account access was not immediately disabled when he resigned. Terminating a network account in a timely manner is an issue of internal communication and procedure and, in mixed Windows/Unix environments, may require a coordinated effort by several teams within IT. While enterprise IdM systems can greatly enhance our ability to react quickly in complex environments, sound policies, procedures and open communication among the business, HR and IT minimize the risk that a terminated employee will come back to bite you.

Two-factor authentication and strong password policy to drive DLP: A laptop belonging to your VP of research and development was just stolen at an industry symposium, and the

Figure 3

Sources of Data Loss

How concerned are you about the following potential sources of data leaks?



Note: Mean average ratings based on a five-point scale, where 1 is "not at all concerned" and 5 is "extremely concerned"

Data: InformationWeek Analytics Data Loss Prevention Survey of 218 business technology professionals



Analytics Report

system contains your product strategy for the next two years along with confidential information regarding potential acquisition targets—definitely not something you want falling into a competitor's hands.

While the laptop is protected by whole-disk encryption software (right?), theoretically, a dictionary attack could crack the cached Active Directory login credentials needed to gain access to files. Thankfully, all your VPs are equipped with two-factor authentication using a product like RSA's tokens, and his token is attached to his keychain, which he does have in his possession.

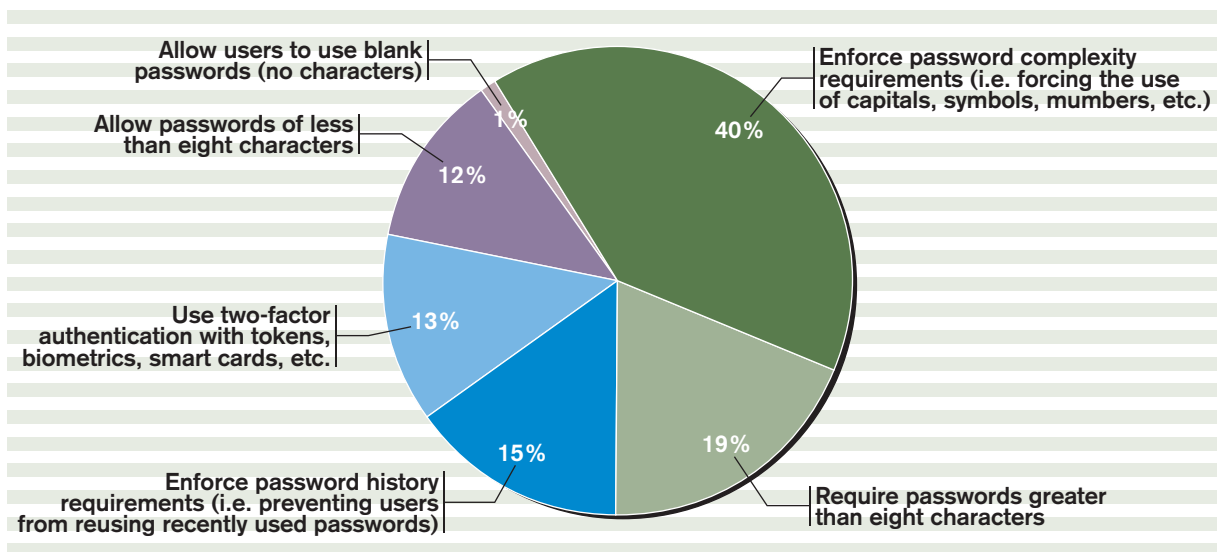
If your IT shop were in this position, would it have been as prepared? Probably not—according to our poll, when asked about the primary measure taken to authenticate identity, only 13% of respondents say they presently employ two-factor authentication.

While this isn't all that surprising given the cost and complexity of doing two-factor, we expect strong growth in this sector as the regulatory landscape gets more complex. A strong authentication infrastructure greatly increases the effectiveness of your other protective systems. To the

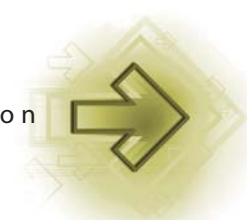
Figure 4

Identity Authentication

What is the primary measure you take to authenticate identity?



Data: InformationWeek Analytics Data Loss Prevention Survey of 218 business technology professionals



Analytics Report

degree budgets and staffing allow, consider two-factor authentication as part of your overall DLP strategy. Tokens and smartcards are the most scalable, enterprise-ready route, but you don't need to invest big dollars. Many business-class laptops come with built-in biometric scanners, for example.

In addition to beefing up your authentication infrastructure, consider simultaneously boosting the strength of your passwords. Not only is a policy requiring strong passwords critical to making yourself a more difficult target to attack, it's something IT can implement with no additional out-of-pocket expense. About 80% of our poll respondents force users to change their password at least every six months, the minimum for best practice purposes.

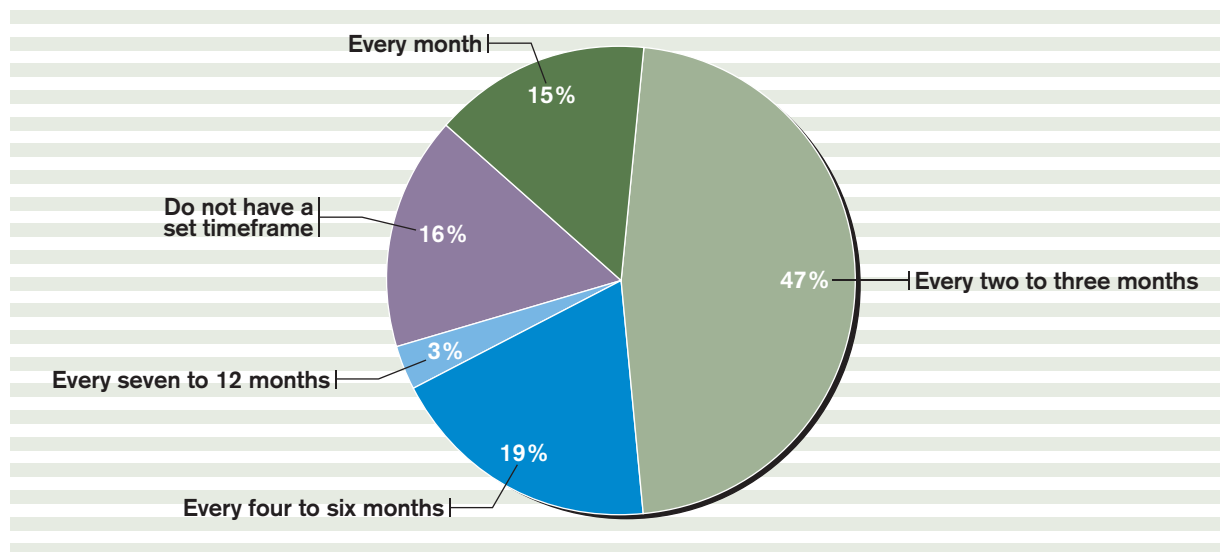
Of course, users dislike strong passwords and aren't afraid to let us know it.

"It drives me nuts that our IT department demands that I change my password every three months, and yet there's nothing sensitive on my laptop," says a director-level poll respondent. "The rare case where I have e-mails about new products, they're very uninteresting compared

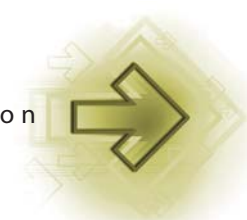
Figure 5

Changing Passwords

How frequently do you require passwords to be changed?



Data: InformationWeek Analytics Data Loss Prevention Survey of 218 business technology professionals



Analytics Report

to our CFO's or possibly VP of HR's systems, which actually have valuable info on them. The policy is so annoying, I go out of my way to make weak passwords."

Security professionals are cringing right now, but this is not an isolated sentiment. The answer is education: Make sure employees know the issue is not just one of protecting the data on their devices, but protecting access to other key systems and networks that their credentials grant.

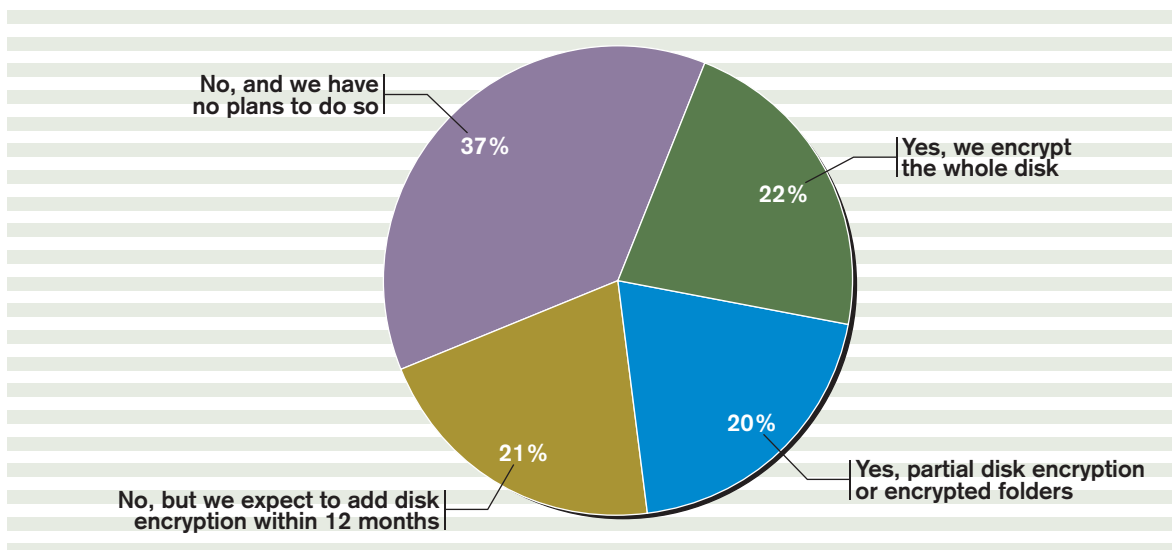
Combine minimum password length, complexity and history requirements with two-factor authentication, and you have a fighting chance at avoiding data loss when systems are lost or stolen. And compliance auditors will surely look upon your diligence with favor.

Tier-1 spyware/malware prevention in a DLP strategy: If anyone asks you what spyware/malware protection has to do with DLP, suggest they call Robert Baldwin, president and CFO of Heartland Payment Systems. Heartland admitted in January that attackers had gained access to systems responsible for processing more than 100 million payment transactions per month, for over 175,000 merchants. The culprit appears to be spyware planted by an insider.

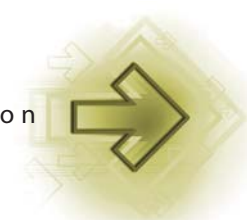
Figure 6

Disk Encryption on Mobile Devices

Does your organization employ disk encryption on laptops, smartphones and other mobile devices?



Data: InformationWeek Analytics Data Loss Prevention Survey of 218 business technology professionals



Analytics Report

To make matters worse, the breach spanned several months, making this data theft incident the largest and most egregious ever recorded—at least at press time.

Detecting and blocking spyware is a particular challenge for smaller companies, which often lack the forensic tools and staff to combat such threats. So what's the best strategy? With budget and staffing concerns out the window, the infrastructure required to implement truly robust prevention of data loss via the spyware vector might resemble the setup in Figure 7, page 17.

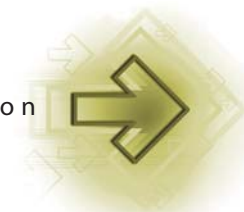
Filtering malware before it gets through the network perimeter is vital, and the best way to do that is with a deep-packet inspection application such as those from Blue Coat, Finjan, Websense and others. We consider desktop malware prevention only somewhat effective, as it's a decentralized protection mechanism that relies on constant updates to maintain its mojo, and it's prone to tampering. Conversely, an inline malware filter is almost tamper proof and provides advanced filtering capabilities coupled with a centralized, single point of policy enforcement for all clients.

What if you already have spyware siphoning off vital data, whether unstructured (Excel spreadsheets or another file format) or from structured databases?

That's where network DLP, enterprise log management and network behavioral analysis earn their keep. Vendors leading the DLP charge include McAfee, RSA, Symantec, Websense and Vericept; all offer a way to fingerprint key data in an effort to detect when an application, user or system is attempting to access or move it.

While network DLP is one very viable answer to detecting the unauthorized movement of structured and unstructured data, it's not foolproof. Fingerprinting data is generally a manual process that requires you to know everywhere critical information is stored—a challenging task in large, complex environments. What happens if spyware taps into a cache of credit card data that's undiscovered and unprotected by your DLP system?

That's where you'll need to go into forensics mode and plug enterprise log management and network behavioral analysis into the mix. LogRhythm and LogLogic lead the charge in the log management space, while Mazu (recently acquired by Riverbed) and Lancopé offer popular network behavioral analysis tools. While the features of these two product genres overlap a tad, each provides a means to document, alert and report on TCP-connection info. For example, you want to know if a server in your data center begins initiating thousands of TCP connec-

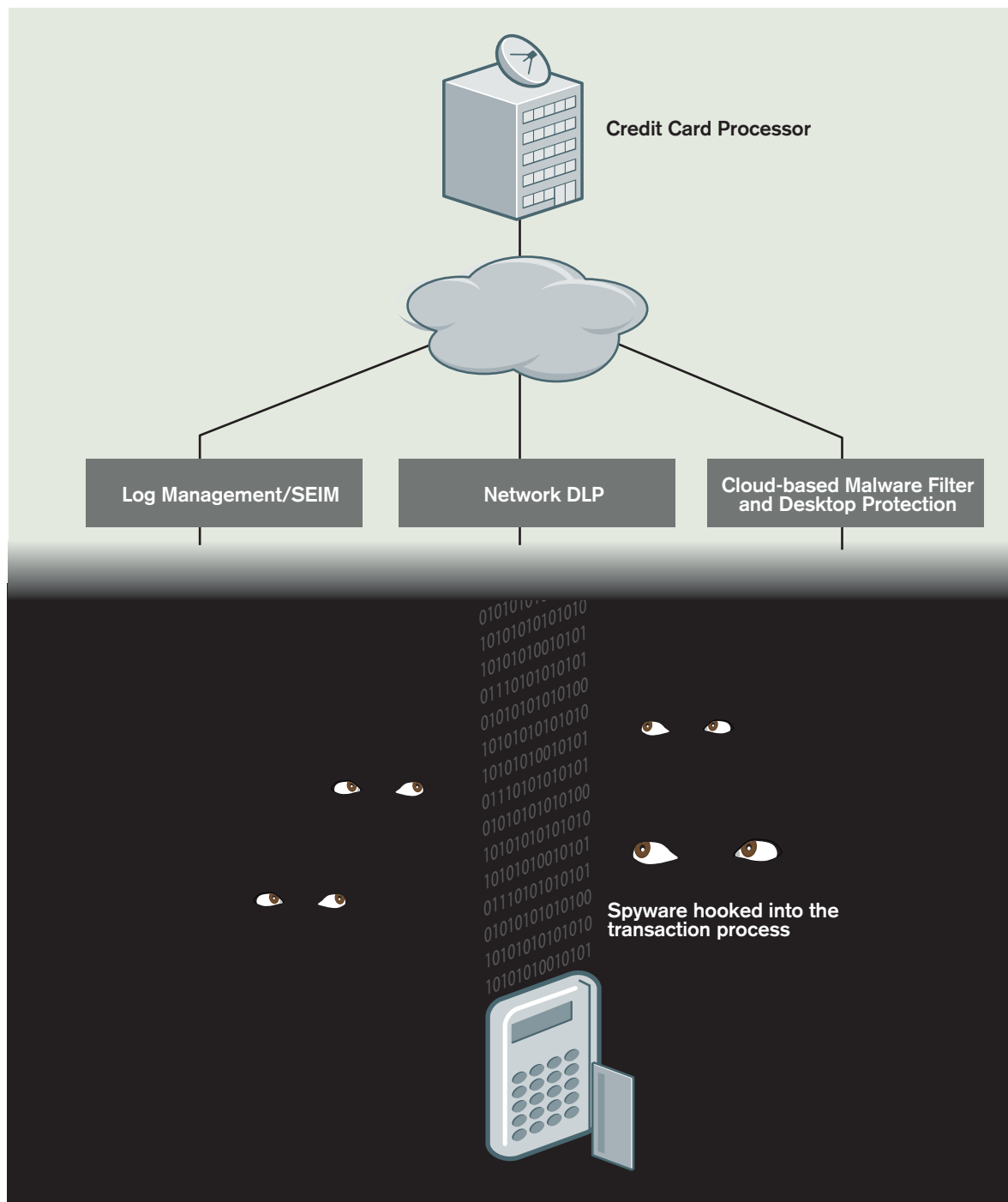


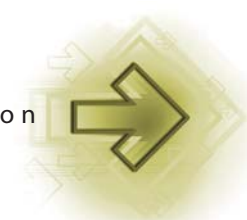
Analytics Report

Figure 7

Prevent, Protect and Prove

A tiered malware defense strategy





Analytics Report

tions per minute to a block of IP addresses hosted in China. At the core of network behavioral analysis is the ability to analyze flow data collected from network devices, among other sources. And while log managers can pull together flow data, they also excel at aggregating a massive amount of log data collected from servers, firewalls, routers and other devices in order to build the forensic trail needed to track and catch intruders.

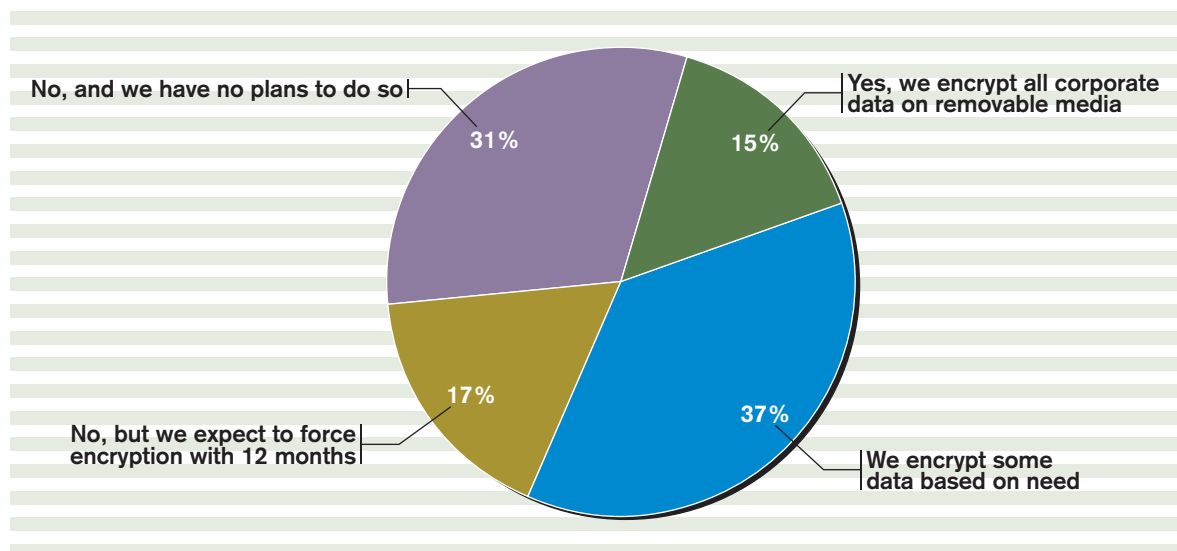
Finally, we want to quickly mention encryption and an up-and-coming technology, endpoint theft deterrence systems. Think of it as LoJack for your laptops, or if that fails, a suicide bomb for the critical data residing on the system that was just stolen—a common scenario by which identify theft happens. Absolute Software provides an app that can track the location of a stolen laptop as well as remotely destroy hard drive content. Whole-disk encryption also goes a long way toward ensuring the integrity of data, assuming you've trained employees not to leave sticky notes with their passwords inside the laptop.

The most important reason for encryption and remote kill switches? Provable verification for auditors that the data on your stolen hardware was inaccessible until it was wiped clean.

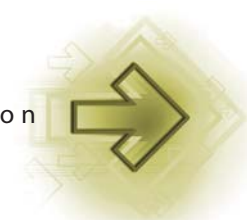
Figure 8

Data Encryption on Removable Media

Does your organization force the encryption of sensitive data on removable media?



Data: InformationWeek Analytics Data Loss Prevention Survey of 218 business technology professionals



Analytics Report

The Genesis of Network DLP

Now that we've laid out a roadmap to execute a robust DLP strategy across several technology genres, let's narrow our focus to analysis of the exploding network DLP space, and most importantly, where these products can help you achieve your data security goals.

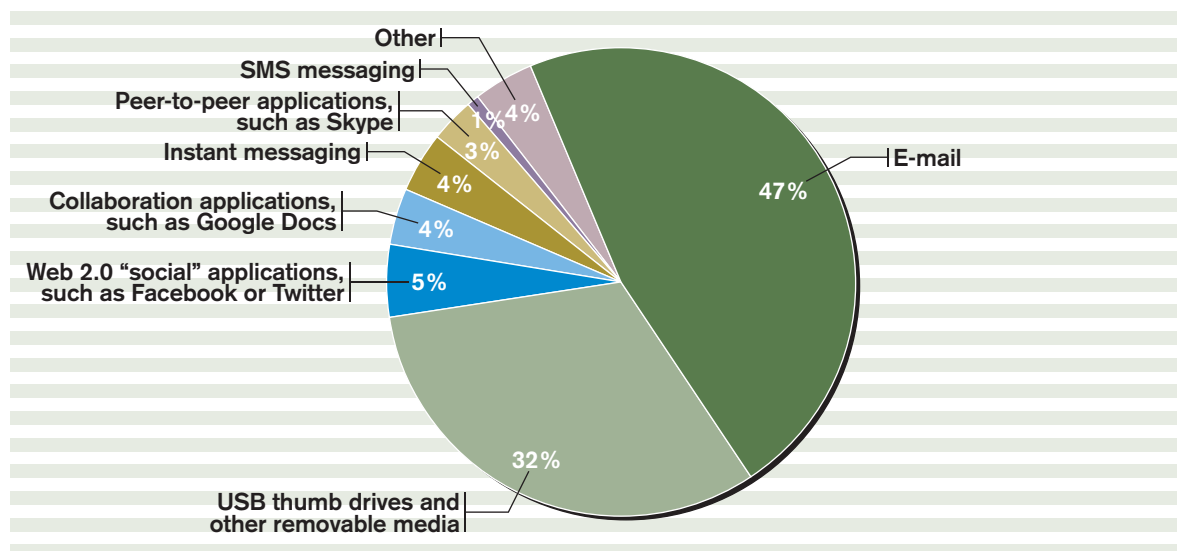
IT managers understand that it's impossible to secure data with 100% certainty. What IT can and must do is assess on a regular basis the most likely and damaging avenues of data loss. Chances are, your primary points of exposure are shared among your peers; here's where *InformationWeek Analytics*' research capabilities benefit you. According to our poll, loss of critical private data contained in e-mail is the single largest concern, with leakage via removable media coming in a fairly close second.

As expected, when we asked what, exactly, IT is most concerned about protecting, the overwhelming majority of responses centered around the type of information you can be sued for losing: PII, consumer credit card and social security numbers, and other types of personal and financial data. Controlling leakage via e-mail is a core capability included in many enterprise

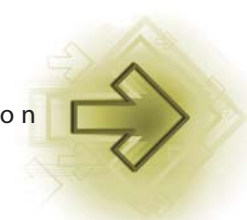
Figure 9

Greatest Risk for Data Loss

Which communication channel presents the single greatest risk for data loss to your organization?



Data: InformationWeek Analytics Data Loss Prevention Survey of 218 business technology professionals



Analytics Report

DLP suites, and later in this report, we'll detail how this technology works, how it's being used today in security-conscious companies, and some of the caveats and pitfalls that one must consider prior to full-scale implementation.

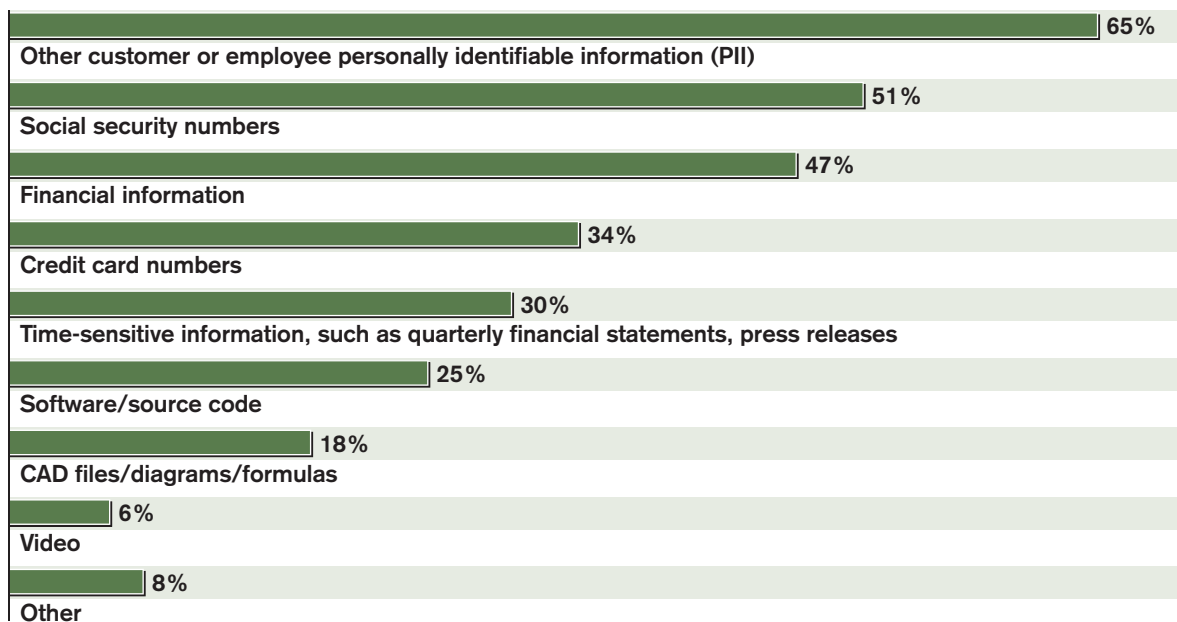
While controlling leakage via e-mail is certainly a high priority, we can't stop there. Essential trade secrets and customer data can just as easily fly out your door via instant messaging, peer-to-peer and Web 2.0 apps, and SMS text messages. Many organizations have the ability to control the use of IM, P2P applications and social networking sites at the gateway, which may be why those security threats represent less of a concern. For example, only 3% of respondents say they're worried about data leakage via peer-to-peer applications.

Are you likely to get sued because your superstar sales executive is chatting with a friend via AOL Instant Messenger? If the discussion relates to whether their next junket is to Nevis or Las Vegas, no. But a sneak preview of your organization's yet-to-be-released annual earnings report

Figure 10

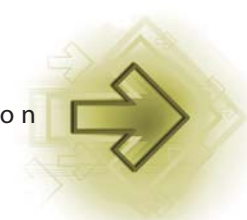
Information Loss Concerns

What types of information are you concerned about leaking?



Note: Multiple responses allowed

Data: InformationWeek Analytics Data Loss Prevention Survey of 218 business technology professionals



Analytics Report

is another matter. DLP systems can watch IM streams, e-mail and other avenues and alert on keywords. The decision is whether to activate that capability, and if so, whether to do nothing but log, monitor for certain keywords and alert, or proactively block messages containing certain phrases. You need to move that discussion to the very top of the organization—tough calls must be made balancing the privacy of employees' communications vs. the need to protect corporate information and digital assets.

The unprecedented visibility into employee communications provided to IT by next-generation DLP tools brings us to our next point.

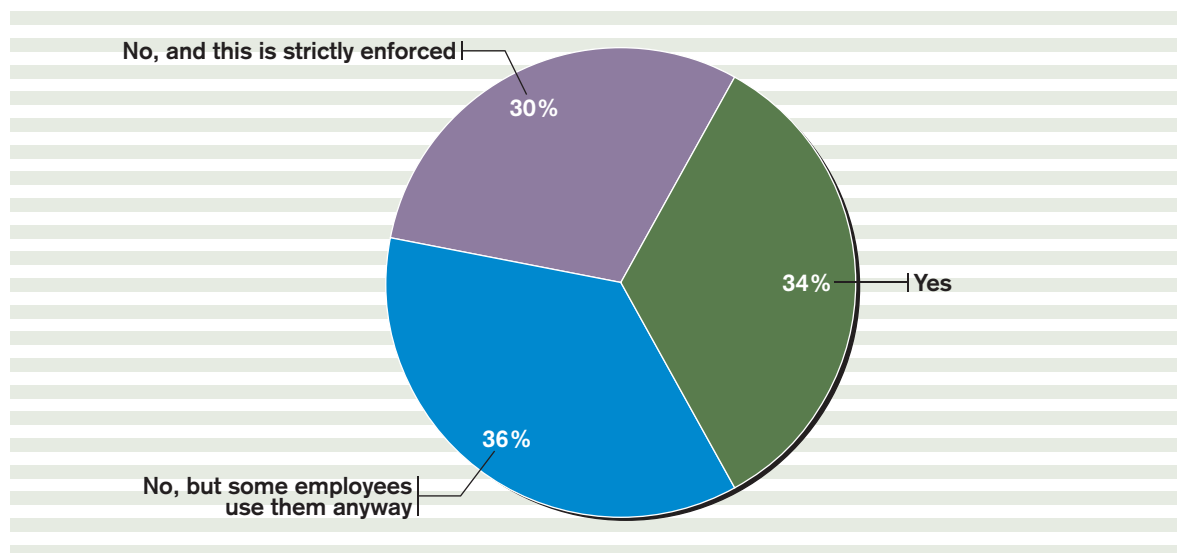
Big Brother Is Watching

In today's highly litigious, highly regulated climate, technology that might have once seemed overly intrusive has become necessary for organizations of all shapes and sizes. Consider the following scenario: The controller for a *Fortune* 500 company is engaged in a heated debate with an analyst over last quarter's results. As part of the conversation, she sends over an attach-

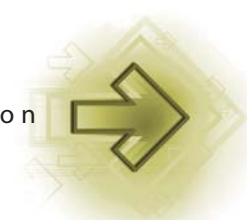
Figure 11

Corporate Use of IM

Does your organization permit the use of consumer instant messaging applications, such as AIM, on corporate devices?



Data: InformationWeek Analytics Data Loss Prevention Survey of 218 business technology professionals



Analytics Report

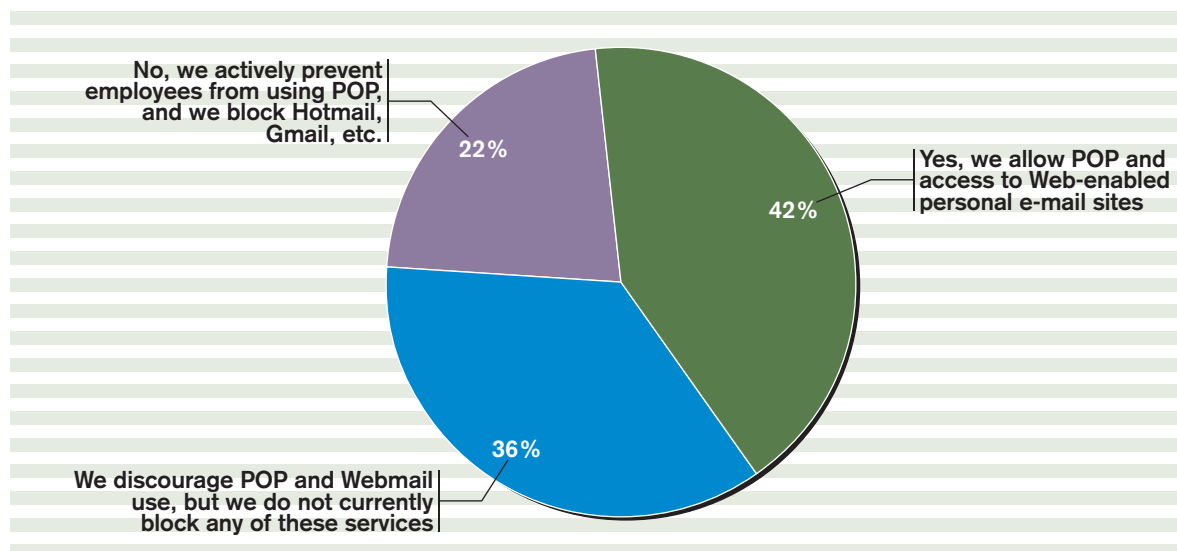
ment containing information intended to illustrate the company's position. The problem is, she realizes after sending the message that she actually attached a confidential memo that spills the beans about a huge account that your corporation might lose this quarter—one that represents 20% of annual revenue. It doesn't matter that the leak was an accident. The fact is, when this information hits the streets, there will likely be a significant sell-off of company stock resulting in millions of dollars in lost net worth.

The outcome of this situation could be very different if IT had DLP technology in place and properly configured. In that case, the controller and her boss would get a call from the CIO saying an outbound e-mail contained an attachment that was fingerprinted by the DLP system and flagged for high-priority review. Human nature being what it is, our controller may well have a sense of anger that IT is scanning her e-mail. Conversely, this technology just saved her job and the company millions, and it might prevent others from making the same mistake. As they consider the pros and cons, most employees will realize that used properly, DLP technology has the potential to do much more good than harm. And pragmatically speaking, the CEO

Figure 12

Personal E-mail Access

Do you allow users POP-based access to personal e-mail accounts from corporate PCs, or allow them to check personal e-mail accounts via Webmail?



Data: InformationWeek Analytics Data Loss Prevention Survey of 218 business technology professionals



Analytics Report

and executive team have an obligation to protect the company, its shareholders and other partners from digital theft and sabotage. Entering stage right are network DLP tools to fill that void.

We asked our survey respondents to rank a list of seven data loss prevention product capabilities from most to least important, whether or not they are currently using or planning to use DLP. Given that e-mail is of the greatest concern as a leakage vector, we weren't surprised to see content security, defined as the ability to scan e-mail and attachments for content that violates policy and take action as necessary, ranked No. 1. We *were* somewhat surprised that data discovery, the ability to crawl all data sources, file shares, e-mail databases and endpoint hard disks for information deemed vital for corporate and customer security, didn't finish higher. When we talk with big IT shops with tight security needs and strict compliance requirements, the ability to perform ad-hoc data discovery is at the top of the list of reasons they give for purchasing or considering a DLP suite.

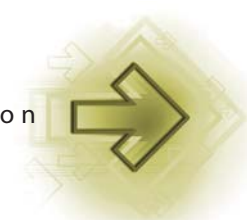
Figure 13

DLP Product Capabilities

Whether or not you are currently using or planning to use DLP, what capabilities would you consider most important to include in a DLP product? Please rank the list of capabilities from 1 to 7, where 1 is the most important capability to have and 7 is the least important.

	Rank
Content security: The ability to scan e-mail and attachments for content that violates policy, and take action as necessary	1
Malware protection: The ability to prevent malware, bots and viruses from stealing critical data over open communication channels	2
Endpoint protection: The ability to report and control data leakage on PCs, laptops and smartphones	3
Enforcement: The ability to block or quarantine actions that would violate policy; for example, stop an e-mail from being sent, or stop data from being copied to removable media	4
Archival: The ability to archive conversations and prevent leakage over non-standard communication channels, such as instant messaging clients or cellular text messages	5
Enterprise data discovery: The ability to crawl all databases, data sources, file shares, e-mail databases and endpoint hard disks for information deemed vital for corporate and customer security	6
Reporting: The ability to report and alert on breaches centrally, with the ability to map certain breaches to regulatory requirements or custom business rules broken	7

Data: InformationWeek Analytics Data Loss Prevention Survey of 218 business technology professionals



Analytics Report

Does this mean that data centers worldwide will begin to implement NSA-like wiretaps of all corporate communications? Of course not, but to the degree that technology allows organizations to manage their exposure to leaks and minimize the risk of lawsuit, you can bet that the insurance policy that is network DLP will continue to gain popularity. The top questions then become, What's the best way to cost-justify DLP in a tight budget season, and what's the best way to implement such protection at the e-mail gateway without interrupting operations with thousands of false positives?

Let's discuss ROI and a few best practices gleaned from our months-long testing of DLP suites.

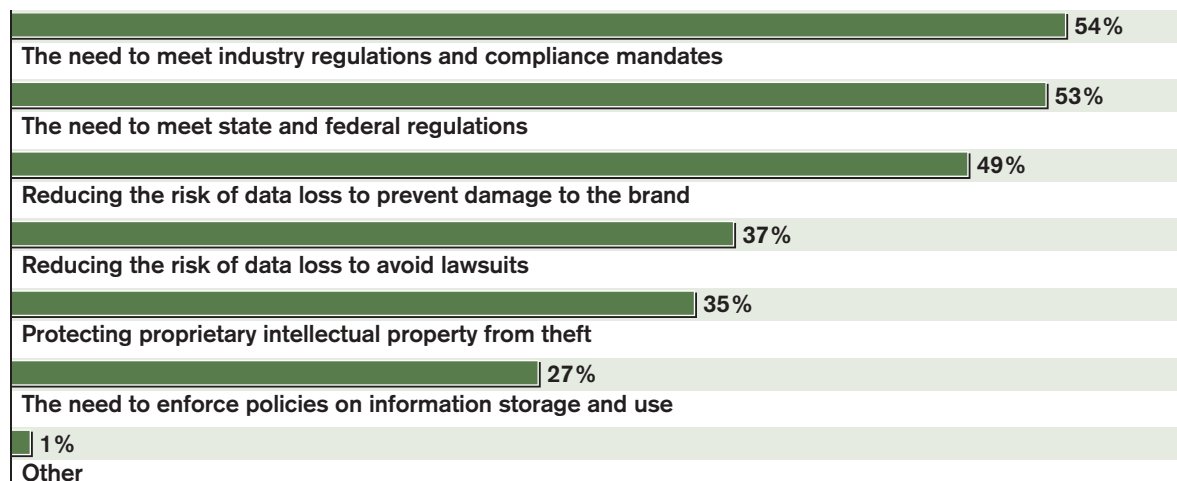
Regulatory Compliance Is Driving This Train

Aggressive growth industries all share one thing in common: a catalyst. Remember when oil hit \$140 in the summer of 2008, or when the price of gas shot past the magic \$4 per gallon barrier? The ensuing outrage sparked a renewed call for conservation and alternative-energy development. In the case of DLP, the catalyst is clearly the outrageously complex and ever-changing regulatory environment in which we all participate. It's not just public companies, health care

Figure 14

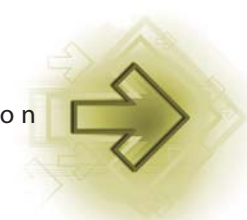
Factors Driving Interest in DLP

What are the top factors that are driving, or would drive, your interest in DLP?



Note: Three responses allowed

Data: InformationWeek Analytics Data Loss Prevention Survey of 218 business technology professionals



Analytics Report

providers and retailers that need to worry about strict data privacy regulations. Increasingly, the small pizzeria owner in Boston and the city librarian in San Francisco also need to pay attention to state-driven data privacy laws.

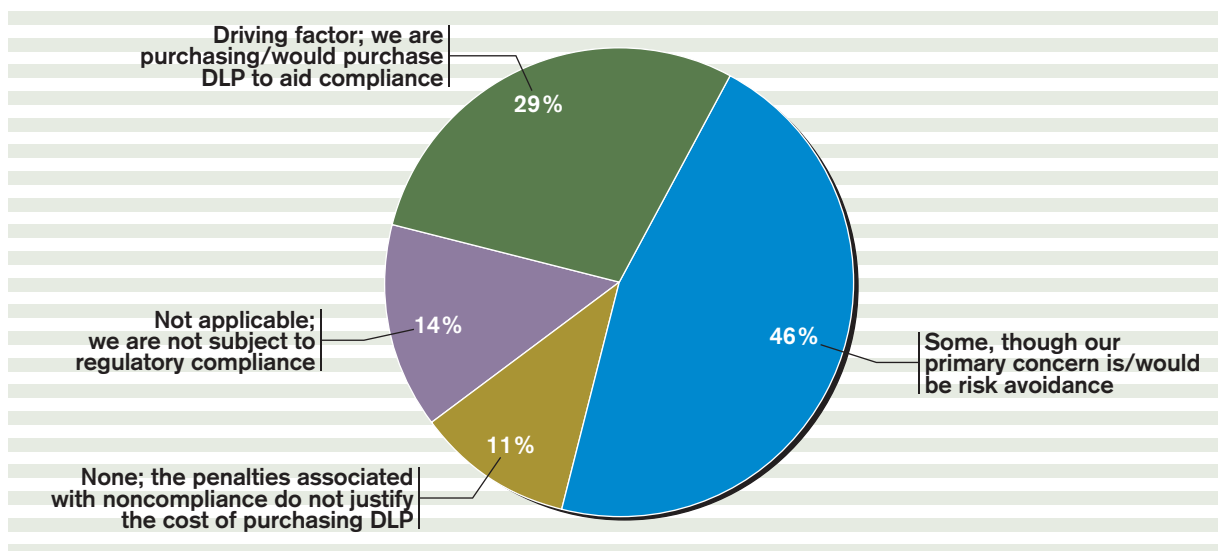
More often than not, according to our poll, the need to facilitate and prove compliance with data privacy or other industry regulations is a top catalyst for purchasing an enterprise DLP package, along with risk avoidance. Just 11% of respondents say the penalties associated with noncompliance do not justify the cost of purchasing DLP, while 14% believe they are not subject to any regulations.

The challenge many enterprises face is matching a broad, and oftentimes vague, set of regulatory requirements to specific DLP features, products and suites. One pertinent example is the new Massachusetts Data Privacy Law. Known to lawyers as 201 CMR 17.00, this relatively new reg is widely believed to be the most far-reaching state-mandated privacy law in the country. While the legislation is a victory for consumer-protection advocates, it's an absolute nightmare

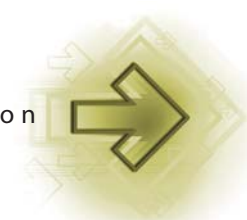
Figure 15

Impact of Compliance on DLP Decision

What role, if any, does, or would, compliance—whether with PCI, HIPAA, state data privacy laws or other regs—play in your decision to purchase or investigate a comprehensive DLP product?



Data: InformationWeek Analytics Data Loss Prevention Survey of 218 business technology professionals



Analytics Report

for IT. Why? The regulations were conceived by legislators who largely have no idea how difficult and costly it is to execute on the myriad vague requirements set forth in the bill—and probably wouldn't care if they did. The enforcement date of CMR 17.00 has been pushed back twice; it's now slated to take effect on January 1, 2010. These delays resulted from push-back from private sector entities confused about how to approach compliance, and concerned with the cost.

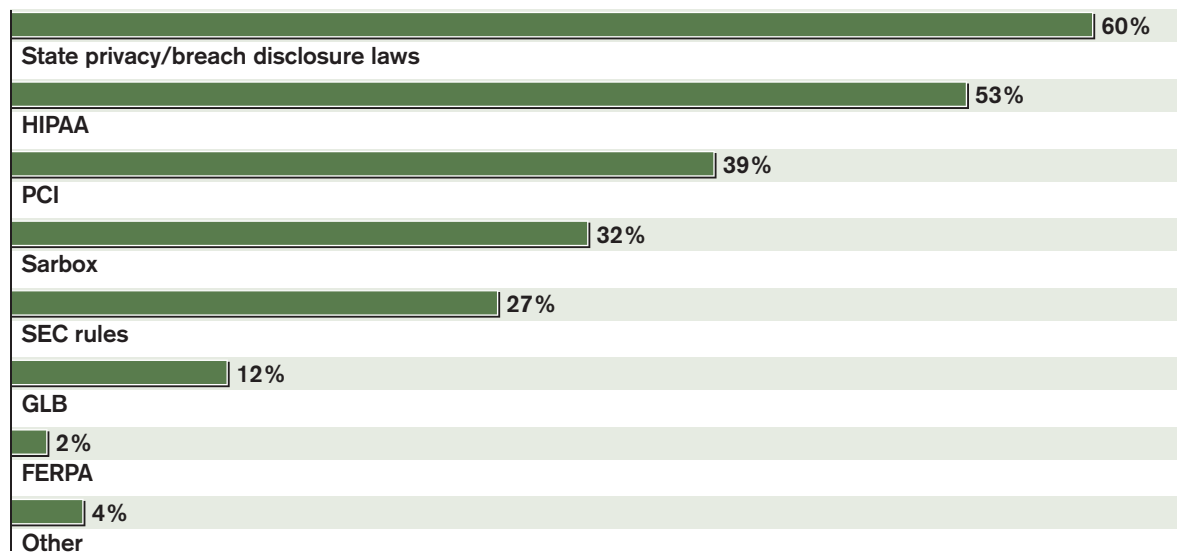
Despite the outcry, we expect more states to adopt laws similar to those in California and Massachusetts. There's also discussion of a national privacy bill. Legislators are hearing loud and clear from constituents that identity theft and credit card fraud are huge issues that need to be addressed. They're tired of companies that they perceive as playing fast and loose with their personal data.

Enterprises that lay the groundwork now for increased government intervention will be ahead of the game. Our strategy for tackling DLP will help.

Figure 16

Satisfying Regulations With DLP

Which regulations do you believe DLP will help you satisfy?



Note: Multiple responses allowed

Base: 165 respondents whose DLP purchase decisions are influenced by compliance regulations

Data: InformationWeek Analytics Data Loss Prevention Survey of 218 business technology professionals



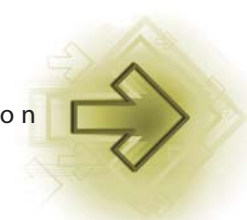
Analytics Report

ROI Analysis: Data Loss Prevention

Our high-level ROI analysis is based on a retailer with 200 employees and 10,000 customer records to protect. Our assumption is that the network/endpoint DLP system prevents one catastrophic data breach over a five-year term; of course, you need to take your particular risk profile into account. In our 2009 Strategic Security survey, 32% of nearly 600 respondents say they expect a breach/espionage within the coming 12 months. How many of those attacks will expose PII is unclear. This analysis assumes a worst-case scenario.

Annual operating expense		
10 man hours per week required for management @ \$50/hour		\$24,000
Product acquisition and maintenance costs		
Capital expenditure		
Network DLP: Code Green CI-1500 Appliance for 200 employees		\$24,000
Endpoint DLP: Optional Endpoint DLP software @ \$14.17/seat * 200		\$2,834
Professional services to install and train staff		\$10,000
Annual maintenance and support		
Support/maintenance for Endpoint+Network DLP @ 18% annually		\$5,010
Total annual cost over five years:		\$36,577
Total cost of ownership of the five-year term:		\$182,884
Cost of data breach*		
Direct and indirect costs of breach response at \$202/record * 10,000	\$2,020,000	
Return on investment assuming a single data breach is prevented		
Total cost of ownership		\$182,884
Amount DLP product saved via prevention of a catastrophic breach	\$1,837,116	
ROI as a percentage	904.5%	

*Our \$202 per record estimate is drawn from Ponemon Institute's latest U.S. Cost of a Data Breach study. The research firm interviewed a large sample pool of data breach victims and discovered that the direct and indirect costs associated with cleaning up a breach average \$202 per customer record lost.



Analytics Report

Strategy for DLP Success From Network to Endpoint

The macro-level factors driving network and endpoint DLP are clear. The question is, as you build your strategy for protecting data and compliance, what range of features are right for your organization?

Although Nick's Pizza Shop does collect credit card data from customers, does Nick need enterprise data discovery capabilities in his DLP system? Clearly not. Conversely, can an international chain like Dominoes meet its security and regulatory requirements with endpoint DLP alone? No way. Most of us fall somewhere in between these two extremes. Before we introduce key features and scenarios that you need to account for in any sound DLP implementation, let's lay out a four-step needs analysis framework.

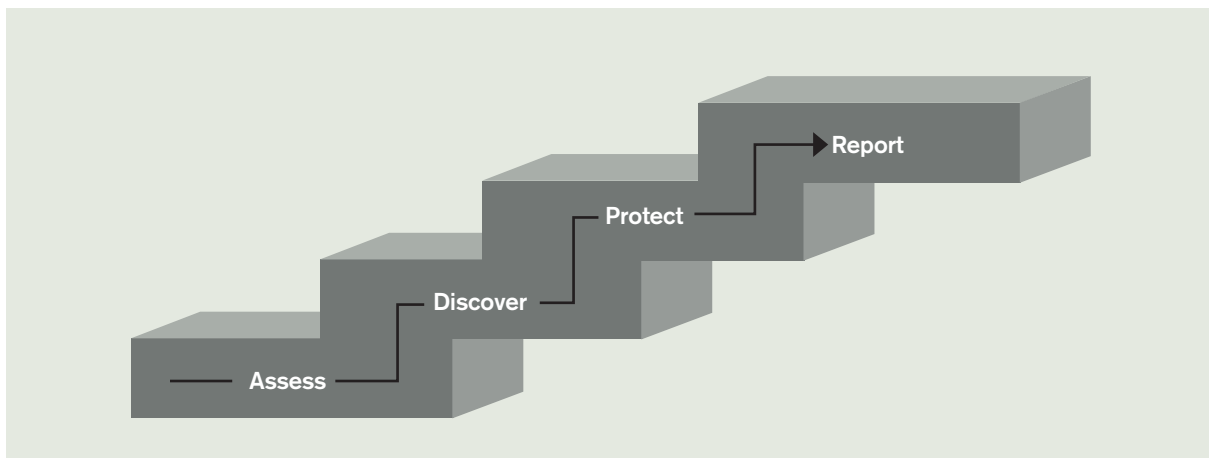
Assessment Phase: At the risk of stating the obvious, the assessment phase is vital to identifying, up front, the goals of your DLP implementation and matching those goals to the feature sets offered by various providers in the DLP space.

Small companies don't generally have to worry about regulations like PCI or the leakage of intellectual property via e-mail, IM or Web applications. As a result, a robust data loss preven-

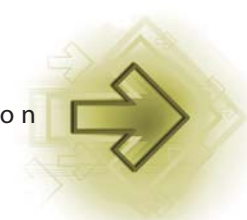
Figure 17

Four-Step Framework for Stopping Data Loss

Developing a data-loss prevention plan tailored for your needs and budget involves a process of assessing loss vectors and compliance requirements, discovering data stores, applying proper protections, then putting ongoing reporting in place for auditing.



Data: InformationWeek Analytics



Analytics Report

tion program can often be accomplished using relatively inexpensive endpoint DLP products coupled with the out-of-the-box capabilities of the Windows operating system.

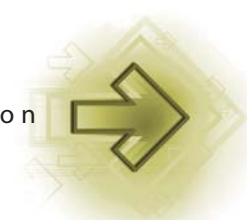
When it comes to endpoint protection, IT shops with high security requirements should consider products that can control access to some or all of the vectors outlined in Figure 18, below.

Figure 18

10 Endpoint Leakage Avenues You Must Block

Vector	Recommendation
Wi-Fi (802.11 a/b/g/n)	For high-value endpoints, prohibit access to unsecured Wi-Fi networks, or disable Wi-Fi entirely.
IrDA (Infrared), Bluetooth	Disable ancillary wireless technologies, like the Bluetooth and infrared ports on laptops, either via a policy-based endpoint DLP suite or other means.
Optical drives	For high-value data, disable the ability to write to optical disk completely. At minimum, force encryption of data when written to disk.
Printing and screen captures	Limit the right to print sensitive data and control where it can be printed. Control the ability to take a screen capture of a sensitive document in an attempt to circumvent security controls. DLP suites can help here.
External USB devices	Secure the use of USB thumb drives and external USB/Firewire drives. Policies enforced by DLP agent software allow admins to essentially disable USB ports, or allow only USB devices registered by IT to be used.
Serial/parallel ports	It requires some skill to use legacy ports to directly leak data, but it's still a threat vector, so disable these ports with your DLP agent software.
Modem	Yes, some people still use analog modems for data/fax. Secure this physical port.
Floppy disk	High-security environments should disable floppy drives completely.
SD cards	Newer laptops have built-in digital card readers that can accept, for example, digital camera memory cards. These devices can be used in the same manner as a thumb drive. Again, DLP agent software can enforce usage policies on these ports.
PCMCIA	Many communication devices still exist for the PCMCIA interface. DLP agents can lock these out as well.

Data: InformationWeek Analytics



Analytics Report

Controlling accidental leaks via the avenues discussed in Figure 18 accounts for only about 25% of the battle, unfortunately, since we're taking into consideration only loss via physical ports on a given endpoint.

Consider the theft or lost-equipment situations discussed in Figure 19, below. While you're in the assessment phase, document these and other real-world situations that could affect your company. Generally speaking, you'll need to combine the capabilities of several technologies to account for all applicable risk situations. Typical endpoint DLP products provide physical-port and usually some level of application control, but not always whole disk or even file-level encryption. You'll also need a separate package to remotely track or send a kill signal to a stolen piece of hardware.

Discovery Phase: Now that you've assessed and prioritized areas of focus for your data loss initiative, it's time to discover just how severe the problem really is. For example, you may believe end users are storing financials on open file shares, which if audited would clearly violate PCI. Or perhaps you suspect employees are carrying confidential intellectual property around on their smartphones.

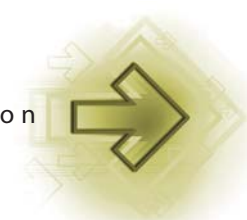
Your mission is to prove it.

Figure 19

3 Endpoint Leakage Scenarios You Must Account For

Scenario	Strategy
Stolen desktop/laptop	The single greatest threat for most organizations. In addition to the need for encryption, IT should consider purchasing a remote kill agent that is capable of verifiable and complete data destruction in the event a high-value laptop is stolen.
Lost Blackberry/smartphone/PDA	Another very high-priority target that should be secured in the same manner as a laptop—encryption and remote kill agents should be loaded before any sensitive data may be placed on the device.
Media theft	Beware of possible data loss via the theft of tapes, USB and optical media. Encrypt, encrypt, encrypt.

Data: InformationWeek Analytics



Analytics Report

Luckily, agentless data discovery of structured and unstructured data sources for compliance reporting is a capability right in the wheelhouse of many leading network DLP systems.

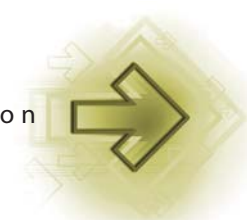
In our testing, Symantec's DLP-9 suite, for example, provided some of the most robust data discovery features we've seen. Need to find out how many clear-text credit card numbers are stored in a particular SQL database, or comb through an entire CIFS or NFS file share looking for spreadsheets that contain social security numbers, or build a complex query that searches for any combination of credit card or social security numbers in a Lotus Notes database? DLP-9

Figure 20

5 Key Network DLP Capabilities

Feature	Strategy
Enterprise data discovery	Enterprises need a centralized tool for determining where critical data resides on the network and on endpoints. Agentless data discovery can scan structured and unstructured data sources, on a scheduled or ad-hoc basis, using Boolean logic to look for particular data patterns, such as spreadsheets that contain credit card or social security numbers, that represent a compliance risk.
Automated quarantine	Leading network DLP suites can ensure compliance by automatically removing any documents uploaded to a file system that violate an administratively defined policy. Make sure the one you shop for can do this.
Digital fingerprinting of data sources	You may have secured a highly confidential contact list against being copied to media, but how do you prevent a malicious attempt to circumvent security through a copy-and-paste action? Network DLP systems can digitally fingerprint data sources. This fingerprint travels with the data, even if it's copied and pasted to a separate file. The fingerprint can then be detected by network DLP if an attempt to transmit, print or copy the data to media is detected.
Pattern-matching discovery within e-mail, IM, Web 2.0	Want an automated alert when an employee e-mails his resume to your competitor? While some might question the rationale for such oversight, network DLP can make quick work of this and other monitoring scenarios. Using Boolean logic, complex queries can be created and attached to outbound data streams for analysis, quarantine or review by management.
Centralized reporting and policy distribution	Reports and security policies pertaining to endpoints and network devices should be centrally aggregated and distributable to all systems. If the product you're considering cannot do this, it should be a deal breaker.

Data: InformationWeek Analytics



Analytics Report

can do it. And Symantec's is not the only suite that distinguished itself in enterprise data discovery during our testing. While we consider a comprehensive data discovery capability a must, there are other key features that should be placed toward the top of your wish list when shopping for a network DLP suite. We discuss these in Figure 20, previous page.

Protect Phase: You've assessed your weak points. You've discovered how your business collects sensitive data, along with how it's stored, distributed and transported. Now you must protect it. Consider doing so along the six key categories we illustrate in Figure 21, below.

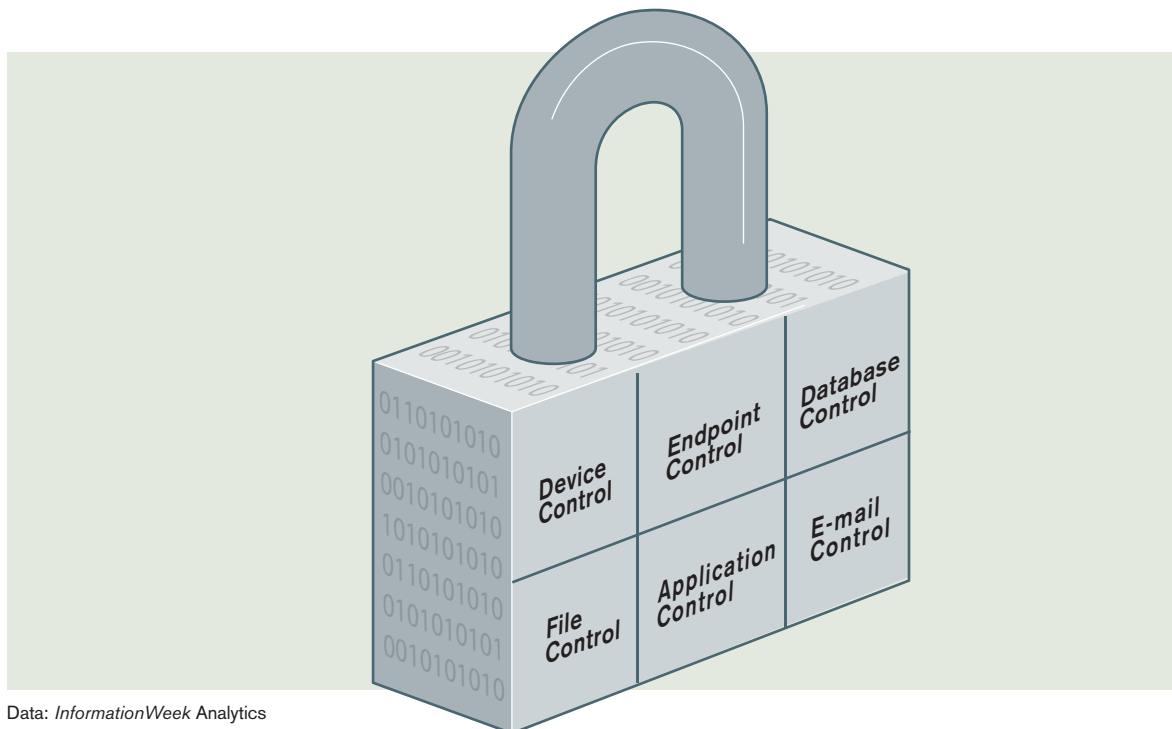
First, determine whether the DLP products you're considering have an answer for securing, auditing, alerting and reporting on various dynamics across these six silos:

Device control: The product should enable IT to robustly manage all devices that data could potentially leak through.

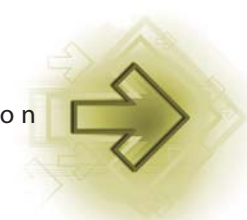
Figure 21

Key Data Protection Controls

There are six main areas where sensitive data may reside. All must be considered when making a protection plan.



Data: InformationWeek Analytics



Analytics Report

Endpoint control: Do you have an answer for encrypting vital data and theft deterrence for hardware?

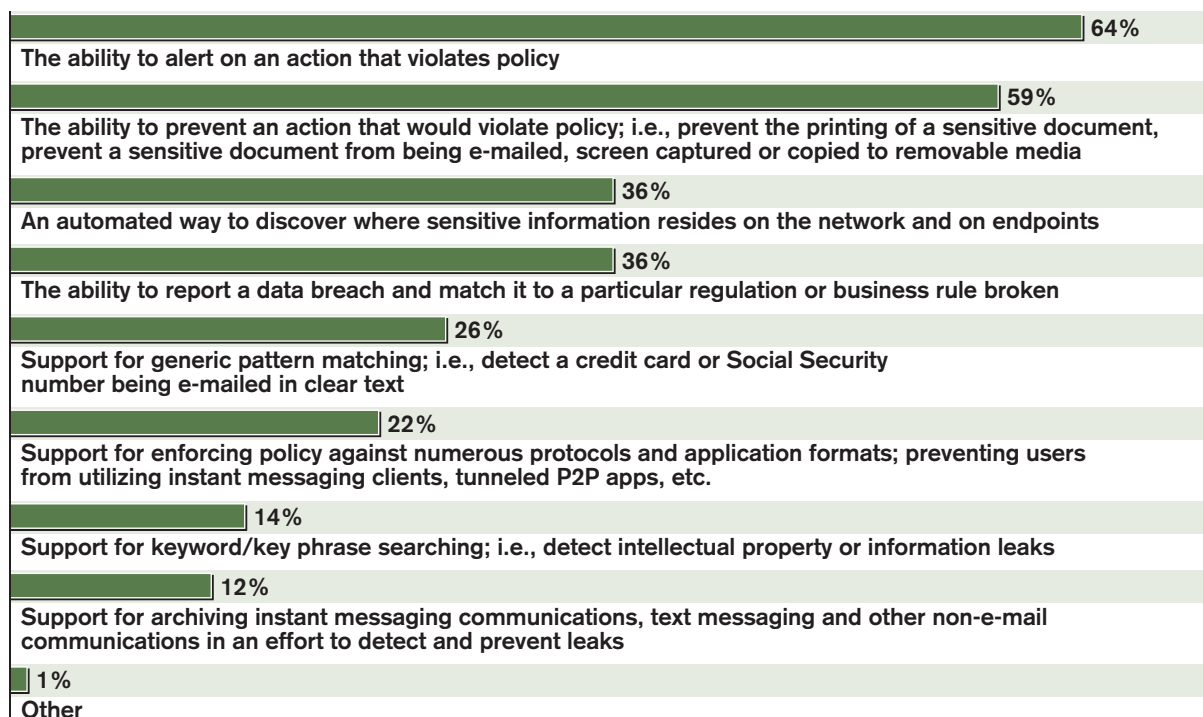
Database control: The product should enable IT to audit and report on database use, access and contents.

File control: Can the suite fingerprint and protect key file data, track usage, block inappropriate transmission and alert/report on policies broken?

Figure 22

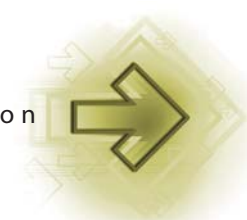
Desired DLP Features

What are the primary features you would want in a DLP product, regardless of your current deployment plans?



Note: Three responses allowed

Data: InformationWeek Analytics Data Loss Prevention Survey of 218 business technology professionals



Analytics Report

Application control: The product should enable IT to control leakage via IM and Web 2.0 applications. Can it block P2P protocols or other applications deemed inappropriate in your environment?

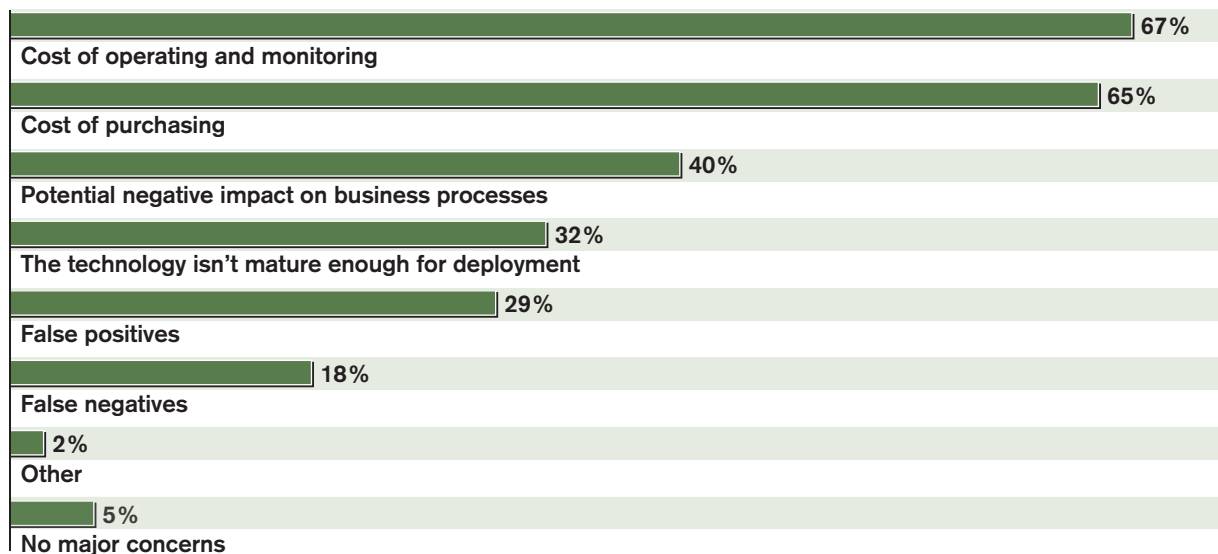
E-mail control: Can you redirect e-mail through the DLP suite for deep content scanning, and can you create complex data-pattern-match queries that help minimize false positives while bringing egregious violations to light quickly?

Reporting Phase: In many ways, this is the most vital. Oftentimes, it's not an issue of whether or not you were able to *stop* an attack, a breach or a data leak. It's a matter of being able to *detect* such an occurrence and report it to the appropriate compliance auditors or law enforcement authorities. Whether that audit is conducted in house or by an independent, external firm is irrelevant. What's vital for minimizing the damage, and resulting publicity fallout, from a leak is that IT have relevant information at its fingertips.

Figure 23

DLP Concerns

What are your primary concerns with DLP technology?



Note: Three responses allowed

Data: InformationWeek Analytics Data Loss Prevention Survey of 218 business technology professionals



A n a l y t i c s R e p o r t

Be sure you can thoroughly report on the happenings within each of the six core security silos discussed above.

We expect sales of DLP products, both network and endpoint, to continue to rise steadily despite economic conditions because of the unique way in which they approach the real-world security issues related to content protection. DLP products, as they're conventionally defined, are still just a single weapon in your arsenal, however. To build a complete data loss prevention infrastructure, add as many of the capabilities discussed in Figure 2, page 11, as possible.

Make your network a tough nut to crack, and most bad guys will shuffle down the road to easier pickings. Beef up your forensic capabilities, and you'll be better prepared to tackle compliance requirements and audits. And most importantly, you'll be ready to go on the offensive against those who challenge your defenses.



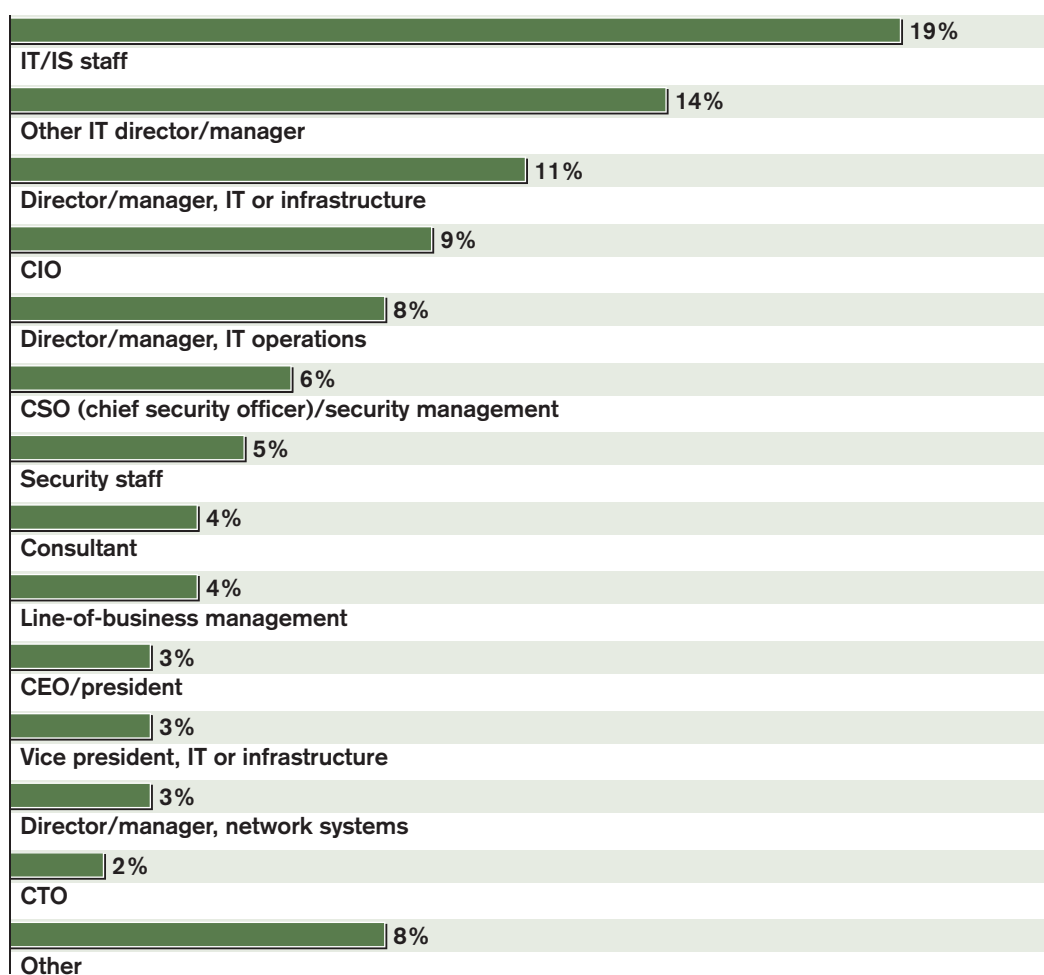
Analytics Report

Appendix

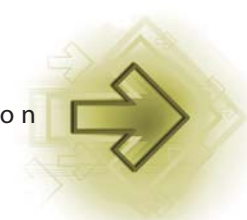
Figure 24

Job Title

Which of the following best describes your job title?



Data: InformationWeek Analytics Data Loss Prevention Survey of 218 business technology professionals



Analytics Report

Figure 25

Will DLP Be a Security Standard?

Do you feel that DLP systems will become a standard security tool in the arsenals of enterprise IT groups?

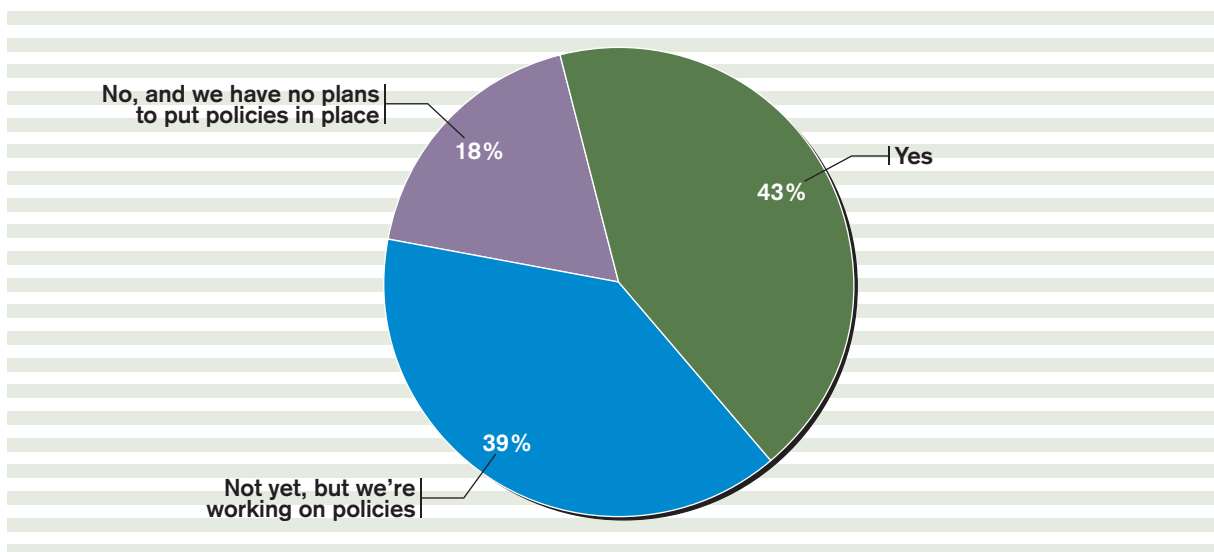
Yes; all large companies will eventually have DLP or answer to auditors	26%
Maybe for some with heavy compliance burdens, but it won't become ubiquitous	60%
Unlikely; while the technology is worthy, it's too complex and/or expensive	12%
No way—even though DLP vendors are shamelessly hyping one security breach after another attempting to drum up sales	2%

Data: InformationWeek Analytics Data Loss Prevention Survey of 218 business technology professionals

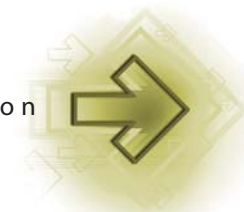
Figure 26

PII Storage Policies

Do you have policies in place that regulate or expressly forbid storing PII or confidential data on personal laptops, removable media and/or smartphones?



Data: InformationWeek Analytics Data Loss Prevention Survey of 218 business technology professionals

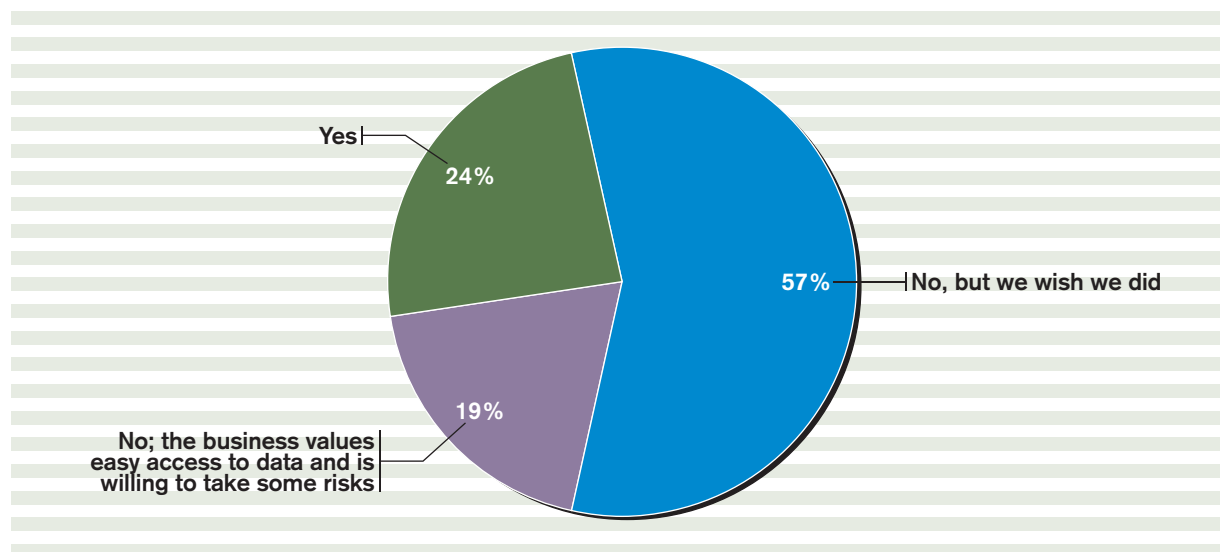


Analytics Report

Figure 27

Technology to Enforce PII Storage Ban?

Whether you have policies or not, do you believe you have the technology in place to enforce a ban on storing PII or confidential data on personal laptops, removable media and/or smartphones?



Data: InformationWeek Analytics Data Loss Prevention Survey of 218 business technology professionals

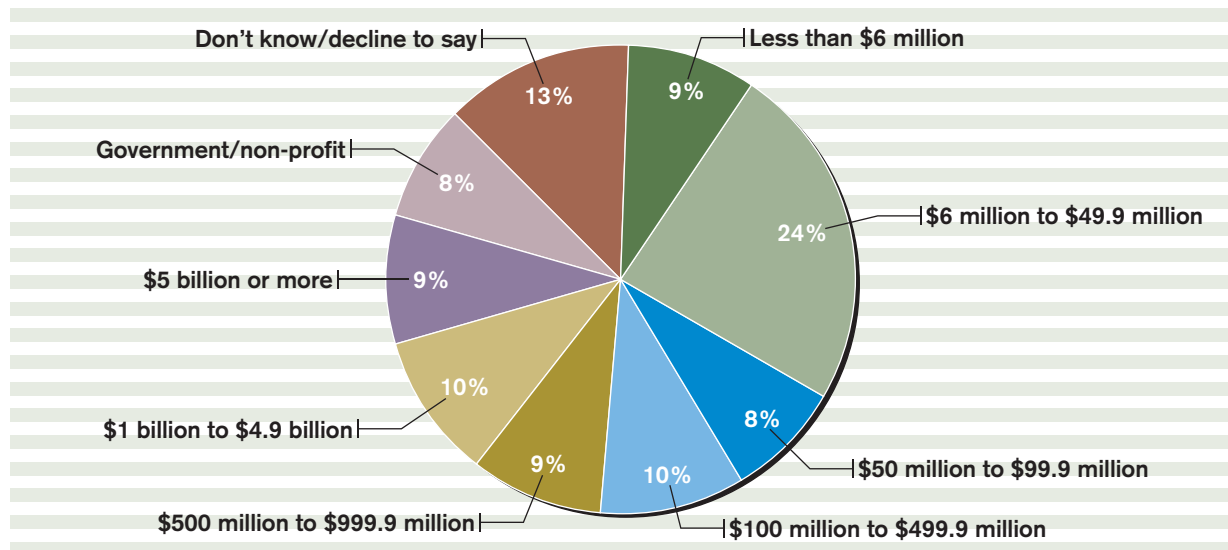


Analytics Report

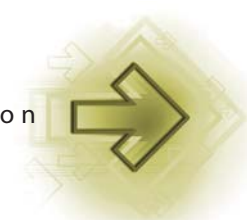
Figure 28

Company Revenue

Which of the following dollar ranges includes the annual revenue of your entire organization?



Data: InformationWeek Analytics Data Loss Prevention Survey of 218 business technology professionals



Analytics Report

Figure 29

Use of Data Loss Prevention

Are you using or considering a DLP product to more granularly control where your organization's critical data travels?

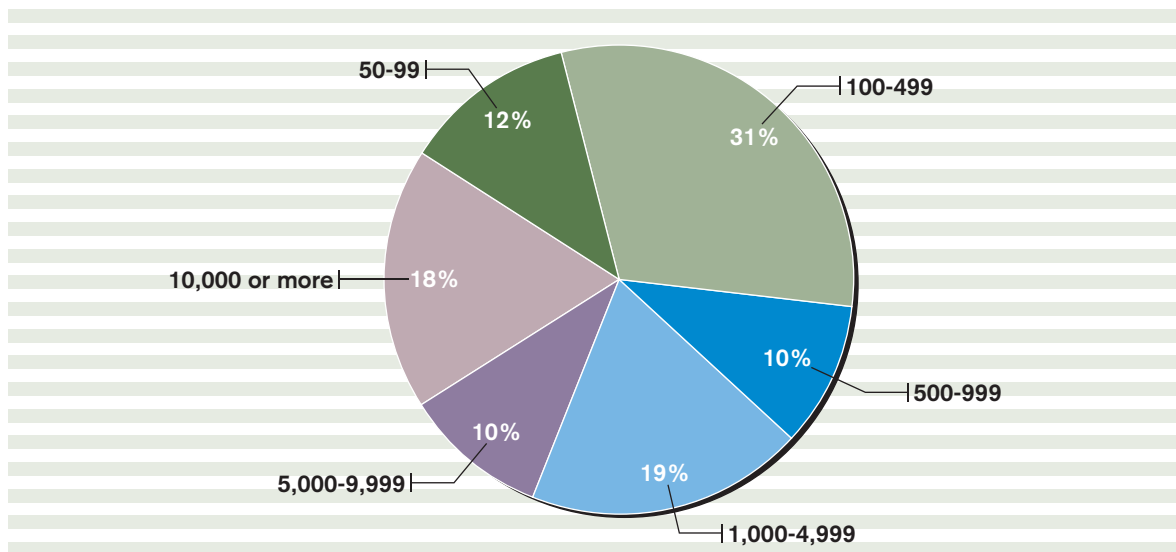
Yes, we have already deployed or are currently deploying	10%
Yes, we plan to purchase within 12 months	7%
Maybe; we're evaluating whether to add DLP to our security mix	36%
No; while the technology is interesting, we feel that our existing security toolset is adequate to protect us from data leakage	25%
No; we don't see enough value in current DLP offerings to make the investment worthwhile	22%

Data: InformationWeek Analytics Data Loss Prevention Survey of 218 business technology professionals

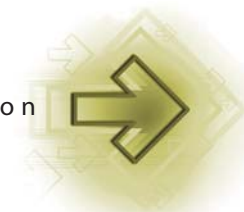
Figure 30

Company Size

Approximately how many employees are in your organization?



Data: InformationWeek Analytics Data Loss Prevention Survey of 218 business technology professionals

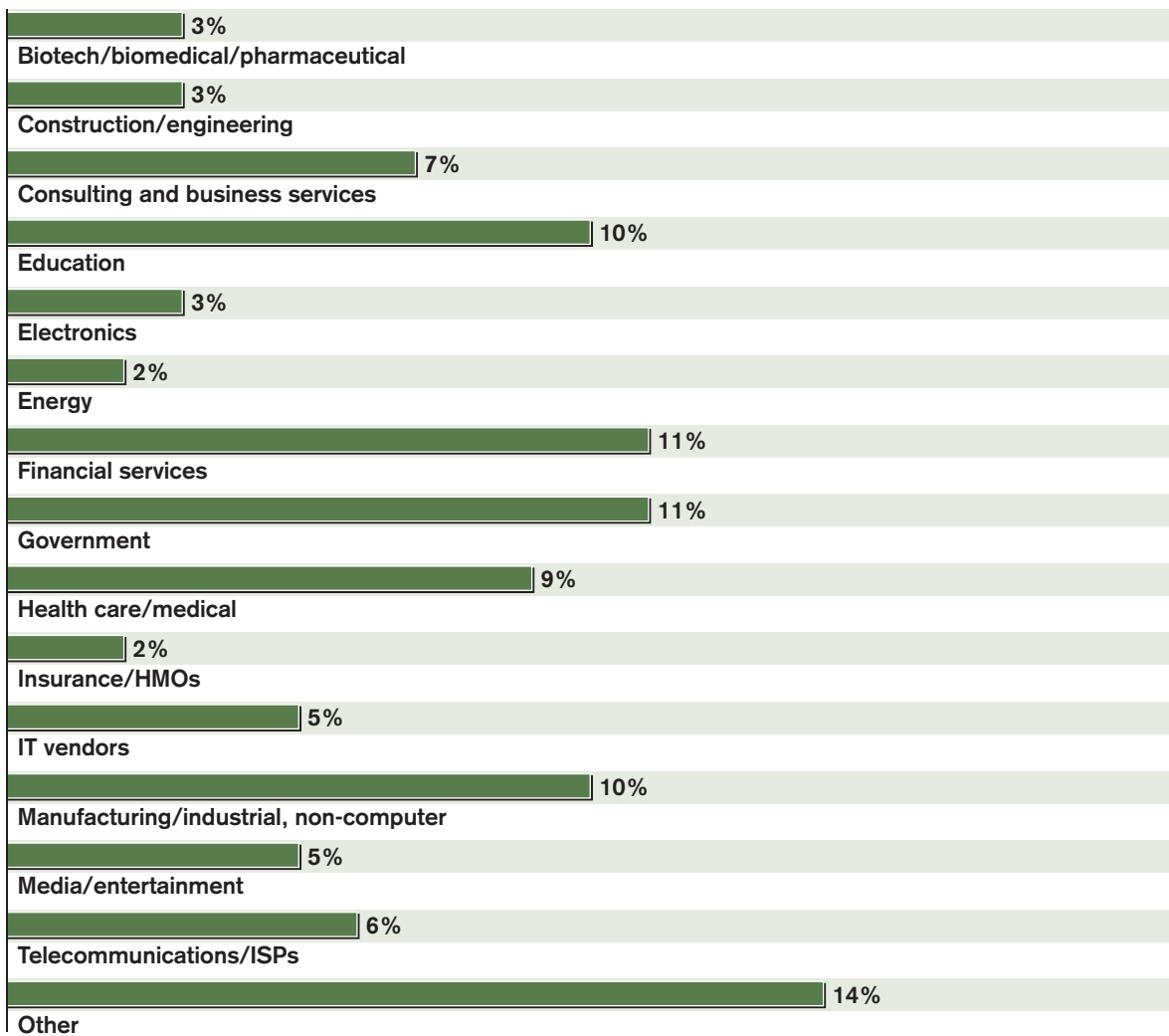


Analytics Report

Figure 31

Industry

What is your organization's primary industry?



Data: InformationWeek Analytics Data Loss Prevention Survey of 218 business technology professionals