January 3, 2012

Rethinking DLP

by John Kindervag

for Security & Risk Professionals

FORRESTER® Making Leaders Successful Every Day

January 3, 2012

Rethinking DLP

Introducing The DLP Maturity Grid

by John Kindervag
with Stephanie Balaouras, Brian W. Hill, and Kelley Mak

EXECUTIVE SUMMARY

Data loss prevention or protection (DLP) — depending upon your usage — is both one of the hottest topics and most difficult challenges among information security professionals today. In 2010, it was the No. 1 security-related search term on Forrester.com, and it continues to represent 20% or more of our 1,600-plus client inquiries each year. However, failed projects and continued challenges have smashed the hope of a DLP technology as a silver bullet that can provide total data security. Using client feedback, survey data, and input from security leaders in Forrester's Security & Risk Council, we looked at DLP with a different lens and realized that security pros needed to approach DLP as an ongoing process, not a product or even a one-time project. We call this new process-based approach "rethinking DLP."

TABLE OF CONTENTS

NOTES & RESOURCES

In developing this report, Forrester drew from a wealth of analyst experience, insight, and research through advisory and inquiry discussions with end users, vendors, and regulators across industry sectors.

Related Research Documents

"Pull Your Head Out Of The Sand And Put It On A Swivel: Introducing Network Analysis And Visibility"
January 24, 2011

"The Forrester Wave™: Data Leak Prevention Suites, Q4 2010"
October 12, 2010

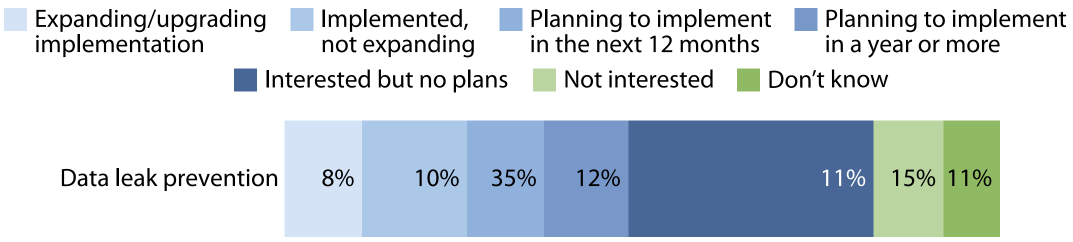
"Introducing The Forrester Information Security Maturity Model"
July 27, 2010

TODAY, DLP ADOPTION IS LOW, OFTEN UNSUCCESSFUL, AND LIMITED IN SCOPE

Currently, the security industry views DLP as a category of *product* — products that detect, and optionally prevent, violations to corporate policies regarding the use, storage, and transmission of sensitive information.[1] Despite 89% of security stakeholders citing data security as their No. 1 challenge, our research indicates that only about one-quarter of enterprise customers have implemented DLP technologies (see Figure 1). Additionally, customer feedback indicates that about half of the companies that have implemented DLP consider those deployments to have failed at some level. Forrester's customers often express frustration with the expectations set by vendors. For example, while a product might find a Social Security Number fairly easily, it becomes a real struggle to identify and protect intellectual property. Also, many deployments take longer than expected and require more resources than anticipated and budgeted for. These changing conditions have left DLP half done in many organizations, thereby creating a level of frustration for project owners.

Figure 1 Enterprise DLP Adoption Is Low

"What are your firm's plans to adopt the following data security and information risk management technologies?"



Base: 1,052 North American and European security decision-makers at companies with 20 or more employees (percentages do not total 100 due to rounding)

Source: Forrsights Security Survey, Q2 2011

61231 Source: Forrester Research, Inc.

Current DLP Deployments Are Limited To Financial Data And PII

When security professionals think of sensitive information, they usually think of two specific data types or use cases. They are: 1) financial information — cardholder data that is subject to PCI requirements or bank account details; and 2) nonpublic personally identifiable information (PII) such as government identifiers — Social Security Numbers in the United States, and personal health information (PHI), which in the United States is subject to HIPAA and HITECH regulations. We estimate these use cases encompass 75% of current DLP deployments (see Figure 2).

There are two reasons that these are the most common DLP use cases. First, these types of data strings (i.e., social security numbers and credit card numbers) are significantly easier to discover and protect using traditional DLP solutions.[2] Second, they're highly regulated. Any company that accepts and stores credit card information is subject to PCI, while a patchwork of federal and local government laws around the globe regulate PII.[3]

Figure 2 A Majority Of DLP Deployments Focus On Financial Data And PII

	75% of use cases	
	Toxic data	**Secrets**
Creator/owner	• Business partners • Customers	Enterprise
Relationship to data	Custodian	Owner
Examples	• Customer PII • Credit card numbers • Government identifiers	• Trade secrets • Strategic plans • Sales forecasts and financials
Source of value	External: determined by regulators and criminals	Internal
Compulsion to protect	Controlled by regulation, statute, or contract	Loss would cause strategic harm
Consequences	Cleanup, notification costs	Revenue losses
Key question	Why is the data circulating?	Who needs to know?
Priorities	• Stop circulation • Reduce use	• Control circulation • Reduce abuse
Domain experts	IT security, legal	Business units

61231

Source: Forrester Research, Inc.

DLP Deployments Overlook The Sensitivity And Economic Value Of Intellectual Property

There are other data types that are often critical to business but are more difficult for traditional DLP tools to detect on their own. Most common is some type of intellectual property (IP). IP includes proprietary data such as earnings forecasts, sales pipelines, strategic plans, trade secrets, and other official data that companies don't want to fall into the hands of their competitors. A growing chorus of government experts suggests that cybercriminals design many of the advanced persistent threat (APT) attacks to steal intellectual property that will advance the interests of nation-states. According to the Office of the National Counterintelligence Executive (ONCIX), "Foreign economic collection and industrial espionage against the United States represent significant and growing threats to the nation's prosperity and security."[4] We estimate that protecting intellectual property represents only 25% of current DLP use cases.

In 2009, Sergey Aleynikov, a vice president and computer programmer at Goldman Sachs, resigned and went to another firm to work on their high-frequency stock trading application. According to the US Attorney's Office, on his last day of work, Aleynikov "transferred substantial portions of Goldman Sachs's proprietary computer code for its trading platform to an outside computer server in Germany.

> "Aleynikov encrypted the files and transferred them over the Internet without informing Goldman Sachs. After transferring the files, Aleynikov deleted the program he used to encrypt the files and deleted his computer's 'bash history,' which records the most recent commands executed on his computer.

> "In addition, throughout his employment at Goldman Sachs, Aleynikov transferred thousands of computer code files related to the firm's proprietary trading program from the firm's computers to his home computers, without the knowledge or authorization of Goldman Sachs. Aleynikov did this by e-mailing the code files from his Goldman Sachs e-mail account to his personal e-mail account, and storing versions of the code files on his home computers, laptop computer, a flash drive, and other storage devices."[5]

Aleynikov was arrested after meeting with his new employer. He was convicted of theft of trade secrets and interstate transportation of stolen property, sentenced to 97 months in prison, and fined $12,500. At sentencing, Judge Denise Cote said, "[Aleynikov's] conduct deserves a significant sentence because the scope of his theft was audacious — motivated solely by greed, and it was characterized by supreme disloyalty to his employer."[6]

Forrester believes that security professionals must start to put a greater emphasis on protecting IP. It's important to protect financial data and PII, but if cybercriminals compromise this data, your company can still recover. The cost to remediate these breaches is high and there could be fines to pay, but your company can still bounce back — just look at TJX Companies and Heartland Payment Systems. However, if a competitor, particularly one sponsored by a nation-state, steals your next-generation product design, the loss of competitive advantage could be permanent.

Over the next few years, expect to see the adoption of other ways to protect and control data that will not be considered part of DLP but that will provide enterprises with a similar result. The most promising technology is the use of encryption to protect intellectual property. Encryption technologies are widely deployed to secure credit card information for meeting PCI compliance objectives.[7] The precedent for excluding encrypted data from data breach notification was set by California SB 1386 and has continued throughout most of the subsequent privacy legislation.[8] If encryption solutions can become easy to scale and manage and inexpensive to use, Forrester anticipates wide adoption of this technology to protect all data types — especially intellectual property.

DLP IS NOT A SINGLE PRODUCT BUT AN EMBEDDED FUNCTION

The low adoption rates, deployments fraught with frustration, and the limited scope of these deployments led Forrester to begin looking at DLP more closely to determine why current solutions were not meeting our customers' expectations. Our findings suggest that too many security professionals approach DLP as one specific product, not a process that looks at data protection holistically and not as a function embedded in multiple security products.

A Single DLP Product Can't Protect All Your Data Loss Channels

Your company can lose data through multiple transport channels — email, web traffic, and instant messaging (IM) — so you must proactively protect each channel. External devices or removable media are also data loss vectors. For example, in the WikiLeaks breach, Private Bradley Manning exfiltrated thousands of sensitive US embassy cables by burning the data to a CD and labeling the disk as a Lady Gaga album.[9] Malicious insiders and cybercriminals may also target FTP sites and databases to gain access to sensitive data. Even well-meaning internal users may inadvertently leak data by losing a laptop or clicking on a seemingly innocuous email attachment that cybercriminals have embedded with hidden malware.

But today, since security professionals think of DLP as a product, many find that they haven't protected all of their data transport channels with DLP technologies. Some DLP solutions focus on one transport channel and not another. Forrester believes that it's very difficult for a single product to protect all channels, and therefore DLP will quickly evolve (if it hasn't already) from a product to a function embedded into multiple (and perhaps all) security products. Forrester has identified five different transport channels that you must protect with DLP technologies. They are:

- **Endpoint.** Endpoint DLP is typically a software agent that looks for out-of-policy data use on endpoints such as laptops and mobile devices. Some endpoint DLP agents may also provide the ability to perform data discovery and classification. Additionally, as mobile devices proliferate, mobile security and mobile device management (MDM) vendors will add DLP functionality.

  Expect to see many endpoint DLP offerings include device control capabilities for controlling data leakage to USB drives and CD/DVD burners. Device control technology has traditionally been a standalone product or has been embedded in antivirus software and endpoint security suites. However, as DLP moves from a product to a function that vendors embed into all manner of products, you should consider endpoint device control solutions as part of DLP. Look for all endpoint DLP software to offer device control solutions that engage with their DLP inspection engines to proactively prevent data leakage via removable devices.[10]

- **Email.** Email DLP is the most mature of the DLP channels. Typically, vendors build DLP control into modern antimalware email gateways. Email DLP got its first big break when healthcare organizations found they needed to encrypt emails containing electronic PHI (ePHI). This led to email encryption engines with lexicons that identified certain prohibited terms or data strings and automatically encrypted those emails. Today, compliance mandates usually require security professionals to encrypt emails containing sensitive or toxic data.

- **Web.** Web DLP looks for data leaks via web channels (HTTP and HTTPS protocols). To do this it must inspect encrypted HTTPS traffic. This requires vendors to build some type of decryption engine into their web DLP solutions.[11] Inspecting SSL/TLS can be problematic from both a technological and privacy perspective. It's generally accepted that security professionals tell users when they inspect their SSL encrypted traffic.

Additionally, web DLP solutions must be bidirectional — they must be able to inspect both the outbound and inbound traffic. Inspecting outbound traffic is especially important in the social web where an individual can post a seemingly innocuous message to a social networking site that will have significant repercussions. Last year, an Israeli soldier unthinkingly posted information about an upcoming military raid. This forced the Israeli army to call off the raid because it feared it had lost the element of surprise.[12] Web DLP solutions must also inspect inbound traffic to protect users from web-based malware often hidden in an innocent looking file that then infects their machines.

- **Gateway.** Gateway DLP solutions were the DLP products that vendors first introduced into the market almost a decade ago. While these solutions were able to provide some data loss uplift for their users, they often promised more than they could deliver. As new threats evolved and cybercriminals discovered new data loss channels, these ubiquitous, all-in-one solutions were not able to meet customers' expectations. From a security professional's perspective, the best solution would be a single appliance to deploy at the egress point — such as a primary Internet connection — and stop all unauthorized data from leaving the organization's boundaries. While this is the endgame of most DLP initiatives, it has not proven a successful model given the multiplicity of extrusion channels that can potentially leak data.

- **Network.** Recently, Forrester defined a new network security space known as network analysis and visibility (NAV).[13] This includes such tools as flow data analysis, metadata analysis, and packet capture analysis. NAV gives security professionals situational awareness in their internal and external network. At the time of the report, we noted an interesting intersection between DLP and NAV and expect to see more NAV vendors add DLP capabilities to their offerings. Currently NAV is focused on visibility — who is doing what and when. However, because NAV tools look at all data moving across inspected network segments, vendors extend these tools to improve data discovery and provide DLP functionality. By using NAV with DLP functionality, security professionals can enable DLP directly on their network and look for data leakage before it reaches other extrusion channels.

FOR DLP TO BE SUCCESSFUL, YOU NEED WELL-DEFINED PROCESSES

Most companies fail in achieving DLP success because they don't define the necessary process and policies before their deployment. DLP tools are not "automagical." They can't find data if they don't know what to look for. Security professionals must train DLP tools by defining policies, but before you can define policies, you have to properly inventory and classify your sensitive information. Our research indicates that most companies don't even know where they have stored their sensitive data and they certainly haven't defined enterprisewide data classification levels such as "top-secret," "company confidential," and "public." This upfront work must be done for several reasons:

- **You need time to build consensus, change internal procedures, and train users.** For the entire history of IT, users have had free rein to use data however they choose. Now, privacy concerns, compliance obligations, and industrial cyberespionage have changed the rules on users. Engage with business leaders, corporate training departments, and human resources to help redefine your culture and make it more security-aware so that you can effectively support a DLP initiative.

- **You must train your DLP tools to protect intellectual property.** As discussed previously, DLP tools can easily discover certain types of data such as Social Security Numbers or credit card numbers because those data strings are known and standardized. However, DLP tools can't find other sensitive information quite so easily. Your DLP solution must be trained to find trade secrets and other intellectual property to know what constitutes this type of data. Computerized technology such as DLP can't intuitively understand most contexts, and therefore, while it's easy for a human to recognize intellectual property data, it can be extremely difficult for a DLP tool to do so and accurately determine data toxicity.

- **You have to carefully decide what business user actions you're willing to block.** The great Catch-22 of DLP is that we need to stop data from leaking outside of our organizational use cases, but at the same time the immaturity of this market makes it difficult — and downright frightening — to actually block data. Most companies find themselves in a monitor only mode — fearful of false positives. But how will you respond if a real breach occurs? Can you catch it in time to significantly reduce its impact? Or will a passive model preclude an agile and rapid response to a potential breach situation? At the very least, have a plan in place to contain any suspected breach, thereby limiting its negative effects.[14]

There Are Five Process Stages To Achieve Before Your Reach DLP Maturity

It can be difficult to tell your DLP tool what data to look for, alert on, or block. To help our customers characterize a more effective DLP process, we've defined five process stages of DLP maturity:

- **Discover.** Data discovery tools and software help enterprises identify the locations of sensitive structured and unstructured information. Its primary goal is to find assets that the enterprise can later classify. Data discovery tools and software are distinct from, but related to, data classifiers. Data discovery tools and software scan endpoints or corporate network assets, such as hosts, database columns and rows, web applications, storage network, and file shares, to identify resources that could contain sensitive information.

- **Classify.** Data classification tools for security parse structured and unstructured data looking for sensitive data that matches predefined patterns or custom policies established by the business.[15] Once matched, data classification tools apply security labels to the information so that tools, such as DLP, can later protect it. It's very important that security professionals work with a cross-functional team of business representatives to define classifications and classification criteria — this is not something that the security department can or should do on its own.

- **Consolidate.** Data consolidation is the process of taking discovered data and aggregating it so that it exists in fewer places, thereby reducing the number of locations that you need to protect. It may also include archiving or deleting data according to company policy. Data consolidation limits your company's exposure to data theft and potentially reduces the scope of compliance, particularly for PCI. You should also consider creating "data free zones" using virtual desktop infrastructure (VDI) encryption, or tokenization. By limiting where toxic data can be stored, companies can simplify the deployment of technology without worrying about potential data loss. This is especially helpful as mobile devices proliferate and IT becomes consumerized.

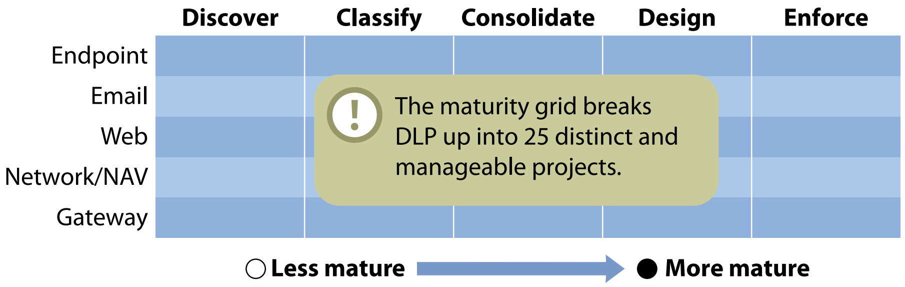
- **Design.** DLP policy design is the process of creating actionable policies that map together data types, classification levels, and DLP tools and technologies for an effective DLP deployment. For example, you have the option to block a user's action if the tool detects a policy violation. However, blocking a user's action can significantly affect his or her productivity and generate ill will toward the security team, especially given the fact that many DLP tools are notorious for false positives. Business unit owners, legal, HR, and other departments must work with security to define no more than three to five classification tiers and only apply the toughest DLP controls to the most sensitive classification tiers.

- **Enforce.** DLP policy enforcement is the process of actually implementing the policy enforcement rules on DLP solutions. For DLP to be truly effective, the DLP tools must proactively enforce the policies defined in the design phase of the project. DLP policy enforcement efficacy can be tracked by leveraging the reports generated by security information management (SIM) or governance, risk, and compliance (GRC) tools. These reports can demonstrate to business leaders that a DLP system is working properly.

ASSESS YOUR DLP DEPLOYMENT USING THE DLP MATURITY GRID

By looking at DLP orthogonally, we can create a grid comparing the five different types of DLP with the five different phases of DLP. This will create a grid that breaks down DLP into 25 distinct and manageable projects that you can assign to members of your team (see Figure 3). By following the DLP maturity grid as a process guide, you can ensure that your DLP team will not skip over critical steps in order to bypass the drudgery that sometimes is inherent in doing things the right way.

Figure 3 The Maturity Grid Makes DLP Manageable



61231 Source: Forrester Research, Inc.

The DLP Maturity Grid Is A Powerful Self-Assessment Tool

Using the DLP maturity grid as a self-assessment tool will allow you to uncover the strengths and weaknesses of both your technology choices and your processes. If you use Forrester's maturity level definitions, which are: 0 — nonexistent; 1 — ad hoc; 2 — repeatable; 3 — defined; 4 — measured; and 5 — optimized, you can tie this DLP maturity exercise back into the Forrester Information Security Maturity Model (see Figure 4).[16]

For example, you might determine that you don't yet have any endpoint DLP deployed but that your email and web DLP solutions are fairly robust. In this situation, you might choose to undergo an endpoint DLP project plus focus on policy design to make your web DLP solution more powerful (see Figure 5).

Figure 4 Tie DLP Into Forrester's Information Security Maturity Model

Level	Characteristics
0 — Nonexistent	Not understood, not formalized, need is not recognized
1 — Ad hoc	Occasional, not consistent, not planned, disorganized
2 — Repeatable	Intuitive, not documented, occurs only when necessary
3 — Defined	Documented, predictable, evaluated occasionally, understood
4 — Measured	Well-managed, formal, often automated, evaluated frequently
5 — Optimized	Continuous and effective, integrated, proactive, usually automated

61231 Source: Forrester Research, Inc.

Figure 5 Use The DLP Maturity Grid To Self-Assess

	Discover	Classify	Consolidate	Design	Enforce
Endpoint	🛇	🛇	🛇	🛇	🛇
Email	◕	◔	◕	◒	◕
Web	◔	◒	◕	○	◔
Network/NAV	○	🛇	🛇	○	🛇
Gateway	○	◔	🛇	◒	○

○ **Less mature** → ● **More mature**

61231 Source: Forrester Research, Inc.

Use The DLP Maturity Grid To Assist In Vendor Selection

The DLP maturity grid is very flexible and will also work for vendor selection. You can interview potential vendors and assign maturity levels to their product to help you make more informed product choices (see Figure 6).

Figure 6 The DLP Maturity Grid Works For Vendor Selection

	Discover	Classify	Consolidate	Design	Enforce
Endpoint	🛇	🛇	🛇	🛇	🛇
Email	●	◔	◕	◒	◕
Web	○	◕	◕	◔	◕
Network/NAV	🛇	🛇	🛇	🛇	🛇
Gateway	○	◔	◕	○	◒

○ **Less mature** → ● **More mature**

61231 Source: Forrester Research, Inc.

RECOMMENDATIONS

REMEMBER THE SIX "P'S" OF DLP

Preventing data from getting into the wrong hands is a key element of information security today. While compliance and regulatory consequences still exist, the rise of organized cybercriminals and the entrance of state-sponsored attacks will put significant pressure on the enterprise to lock down data, especially intellectual property, more effectively. There are six "P's" that companies can look to for guidance when crafting a data-centric security perspective. They are:

- **Priorities.** Start with the highest-value data types first. You should prioritize intellectual property first — data loss that will result in permanent loss of competitive advantage. Next, prioritize financial data and PII — data loss that will result in fees, fines, lawsuits, and damage to corporate reputation.
- **Process.** Start at the beginning and end at the end. By using Forrester's DLP maturity grid you can define an effective process that will help you approach DLP nirvana.
- **Partners.** There are multiple stakeholders involved in any DLP project. Particularly in the development of classification levels and policies, you must partner with HR, legal, IT ops, and compliance teams to build effective partnerships and distribute the burden of DLP. You must also work with HR to determine what action the organization will take to deal with policy violations.
- **Precision.** Be specific about data types, classification, and data owners. Remember that computer programs don't have a "gut-instinct," so you must be as precise as possible in order to effectively deploy DLP. A new product design rendered in AutoCAD is clearly sensitive intellectual property to anyone on the design team. That knowledge is intuitive to humans. But to a DLP engine, that file is merely another .dxf file. The DLP tool must be told that certain specific .dxf files are sensitive so it knows to alert or block appropriately.
- **Patience.** Data-centric security is not just a technological issue but a cultural issue. Cultural change takes time. Most companies have had free rein regarding their data security practices. Be patient as threats, compliance, and customer expectations coincidentally converge to pressure organizations into adopting new data centric strategies.
- **Privacy.** Ultimately, outside forces will mandate how you deal with PII data. As privacy issues become top of mind for governments and users, you should expect more restrictive measures and regulations in the future.

WHAT IT MEANS

DLP IS A PART OF A BROADER INFORMATION RISK AND CONTROL STRATEGY

There are many types of information risks including regulatory noncompliance, legal discovery, operational data loss from IT failures and disasters, and loss of sensitive data. Addressing these various risks is the key to effective security in a very dangerous world. As more data is created and more people and devices get access to this data, the challenge of controlling this data will grow exponentially. The DLP maturity grid provides a good first step in the long-term data control strategies that enterprises will need to create over the next few years. This strategic initiative usually requires that the organization take a step back in order to discover or inventory its data, classify it based on sensitivity and criticality to the business, and then determine an appropriate course of action based on the organization's risk tolerance. There are many opportunities across IT silos including information management professionals, IT operations professionals, and security professionals to come together to consolidate processes like discovery and classification.

There are also areas where one department's priorities will pass on benefits to the other. Archiving is a good example. Archiving data is critical to meeting certain regulatory and legal discovery requirements. For IT operations, archiving large data volumes from production systems improves the performance of these systems. For security professionals, archiving means there is less sensitive data lying around unprotected.

SUPPLEMENTAL MATERIAL

Methodology

Forrester's Forrsights Security Survey, Q2 2011, was fielded to 2,353 IT executives and technology decision-makers located in Canada, France, Germany, the UK, and the US from small and medium-size business (SMB) and enterprise companies with two or more employees. This survey is part of Forrester's Forrsights for Business Technology and was fielded during June 2011. LinkedIn Research Network fielded this survey online on behalf of Forrester. Survey respondent incentives included a choice of gift certificates and charitable donations. We have provided exact sample sizes in this report on a question-by-question basis.

Forrester's Forrsights for Business Technology fields 10 business-to-business technology studies in 12 countries each calendar year. For quality control, we carefully screen respondents according to job title and function. Forrester's Forrsights for Business Technology ensures that the final survey population contains only those with significant involvement in the planning, funding, and purchasing of IT products and services. Additionally, we set quotas for company size (number of employees) and industry as a means of controlling the data distribution and establishing alignment with IT spend calculated by Forrester analysts.

ENDNOTES

[1] Forrester first began to define DLP within the context of our clients' experience. For more information, see the February 10, 2009, "Inquiry Spotlight: Data Leak Prevention, Q1 2009" report.

[2] The most common form of DLP looks for this type of sensitive data using Regular Expressions (RegEx) to compare known string types — say a credit card number — with data strings seen within a packet. When the data strings match, the DLP tool can query its policy engine and take a particular action such as notify a data owner or even perhaps block the data from exiting the environment.

[3] For more information on privacy laws, see the April 21, 2011, "The Privacy Almanac Series: Establishing A Privacy Framework" report.

[4] The Office of the National Counterintelligence Executive (ONCIX) issues annual reports on foreign economic and industrial espionage. Source: Office of the National Counterintelligence Executive (http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf).

[5] Source: "Manhattan U.S. Attorney Charges Former Goldman Sachs Computer Programmer For Theft Of Trade Secrets," Computer Crime & Intellectual Property Section press release, February 11, 2010 (http://www.cybercrime.gov/aleynikovChar.pdf); *The Wall Street Journal* (http://online.wsj.com/public/resources/documents/021110aleynikovindictment.pdf).

[6] For more information on the sentencing of Sergey Aleynikov, read the press release on the United States Department of Justice website. Source: "Former Goldman Sachs Computer Programmer Sentenced In Manhattan Federal Court To 97 Months In Prison For Stealing Firm's Trade Secrets," The United States Department of Justice press release, March 18, 2011 (http://www.justice.gov/usao/nys/pressreleases/March11/aleynikovsergeysentencingpr.pdf).

[7] For more information on encrypting credit cards, see the April 7, 2010, "Demystifying Tokenization And Transaction Encryption, Part 1: Get Ready To Place Some Bets" report.

[8] California SB 1386 requires "a state agency, or a person or business that conducts business in California, that owns or licenses computerized data that includes personal information, as defined, to disclose in specified ways, any breach of the security of the data, as defined, to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person." Source: "SB 1386," State of California (info.sen.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.html).

[9] For more information on the WikiLeaks/Bradley Manning breach, see the January 24, 2011, "Pull Your Head Out Of The Sand And Put It On A Swivel: Introducing Network Analysis And Visibility" report.

[10] This type of software looks at the data that the user is attempting to move to the removable device, and by comparing this data with the policy defined in the DLP engine it will typically allow, deny, or encrypt the data transfer to the device.

[11] The vendor typically installs an X.509 SSL on the gateway, so that they can perform a "man-in-the-middle" type of attack on the encrypted stream that enables them to inspect that traffic for data leakage policy violations.

[12] Source: Haaretz Service and Reuters, "IDF calls off West Bank raid due to Facebook leak," *Haaretz.com*, March 3, 2010 (http://www.haaretz.com/news/idf-calls-off-west-bank-raid-due-to-facebook-leak-1.264065).

[13] For more information, see the January 24, 2011, "Pull Your Head Out Of The Sand And Put It On A Swivel: Introducing Network Analysis And Visibility" report.

[14] For more information on potential incident response options, see the November 9, 2011, "Planning For Failure" report.

[15] Data classification tools generally look for data that it can match deterministically, such as credit card numbers or US Social Security Numbers. Some data classification tools also use fuzzy logic, syntactic analysis, and other techniques to classify less structured information.

[16] Forrester's Security Maturity Model is a powerful tool to track the maturity of your security organization. See the July 27, 2010, "Introducing The Forrester Information Security Maturity Model" report.

FORRESTER®

Making Leaders Successful Every Day

Headquarters

Forrester Research, Inc.
60 Acorn Park Drive
Cambridge, MA 02140 USA
Tel: +1 617.613.6000
Fax: +1 617.613.5000
Email: forrester@forrester.com
Nasdaq symbol: FORR
www.forrester.com

Research and Sales Offices

Forrester has research centers and sales offices in more than 27 cities internationally, including Amsterdam, Netherlands; Beijing, China; Cambridge, Mass.; Dallas, Texas; Dubai, United Arab Emirates; Frankfurt, Germany; London, UK; New Delhi, India; San Francisco, Calif.; Sydney, Australia; Tel Aviv, Israel; and Toronto, Canada.

For the location of the Forrester office nearest you, please visit: www.forrester.com/locations.

For information on hard-copy or electronic reprints, please contact Client Support at +1 866.367.7378, +1 617.613.5730, or clientsupport@forrester.com. We offer quantity discounts and special pricing for academic and nonprofit institutions.

Forrester Research, Inc. (Nasdaq: FORR) is an independent research company that provides pragmatic and forward-thinking advice to global leaders in business and technology. Forrester works with professionals in 19 key roles at major companies providing proprietary research, customer insight, consulting, events, and peer-to-peer executive programs. For more than 28 years, Forrester has been making IT, marketing, and technology industry leaders successful every day. For more information, visit www.forrester.com.

FORRESTER®