

Data Loss Prevention

Little Leaks Sink the Ship

May 2008

~ Underwritten, in Part, by ~



The Security Division of EMC



Executive Summary

This report is a guideline for organizations interested in data loss prevention ("DLP") solutions as part of an overall strategy for protecting sensitive data.

Best-in-Class Performance

To distinguish Best-in-Class companies from Industry Average and Laggard organizations, Aberdeen used the year-over-year changes in the following performance criteria:

- Number of data loss incidents
- Number of non-compliance incidents (e.g., failed audits) related to data protection
- Amount of human error related to data protection
- Number of help desk calls related to data protection

Companies with top performance based on these criteria earned Best-in-Class status.

Competitive Maturity Assessment

Survey results show that the firms enjoying Best-in-Class performance shared several common characteristics, including the following:

- 50% have discovered and classified their information assets
- 64% have established consistent policies for protecting data at rest in back-end systems, data in transit, and data in use at the endpoints
- 64% have automated the enforcement of their data protection policies, unaided by the end-users (48% provide real-time alerts and notifications to their end-users)
- 68% have effective measurement of the information required for governance of their data protection initiatives, including the number and source (channel, and user) of data loss incidents
- 59% have formal documentation, awareness and end-user training programs regarding their data protection policies
- 67% have deployed e-mail and web monitoring and filtering solutions; 41% have deployed network-based DLP; 32% have deployed agent/endpoint-based DLP; 73% have deployed some form of encryption at the endpoint

Recommended Actions

In addition to the specific recommendations in Chapter Three of this report, to achieve Best-in-Class performance companies should view DLP solutions as important elements of an information-centric strategy to identify, classify, protect, and manage sensitive information.

Research Benchmark

Aberdeen's Research Benchmarks provide an in-depth look into process, procedure, methodologies, and technologies; identify best practices; and make actionable recommendations

"DLP solutions don't have to be that pretty. The most important thing is that they are accurate, and that they are unobtrusive. The referee can be ugly, as long as he makes good calls, doesn't make bad calls, and lets the game go on."

~ VP and Business Unit Manager, mid-size enterprise

Send to a Friend 

Table of Contents

Executive Summary.....	2
Best-in-Class Performance.....	2
Competitive Maturity Assessment.....	2
Recommended Actions.....	2
Chapter One: Benchmarking the Best-in-Class.....	5
Business Context: Data, Data Everywhere.....	5
Aberdeen's Maturity Class Framework.....	8
Best-in-Class PACE Model.....	9
Best-in-Class Strategies.....	9
Chapter Two: Benchmarking Requirements for Success.....	12
Competitive Assessment.....	13
Capabilities and Enablers.....	14
Chapter Three: Recommended Actions.....	22
Laggard Steps to Success.....	22
Industry Average Steps to Success.....	22
Best-in-Class Steps to Success.....	23
Appendix A: Research Methodology.....	24
Appendix B: Related Aberdeen Research.....	26
Featured Underwriters.....	27

Figures

Figure 1: Standards and Best Practices with Highest Impact on Incremental Investments in DLP (1 = Lowest, 5 = Highest).....	5
Figure 2: Managing Expansion of Access to Sensitive Information (% of companies reporting year-over-year increase).....	6
Figure 3: Data Loss Incidents in the Last 12 Months, by Type (indexed to Industry Average = 1.0).....	7
Figure 4: Top Pressures Driving Current Investments in DLP.....	10
Figure 5: Leading Strategies Driving Current Investments in DLP.....	10
Figure 6: Classification is the Foundation for Consistent Policies.....	15
Figure 7: Systematic Rollout and Proactive Management.....	15
Figure 8: One Throat to Choke; Educated End-Users.....	16
Figure 9: Visibility into Key Data and Intelligence.....	17
Figure 10: Many Approaches to Automated Enforcement of Data Protection Policies.....	17
Figure 11: Enabling Technologies – Monitoring and Filtering.....	18
Figure 12: Enabling Technologies – Encryption.....	19
Figure 13: Enabling Technologies – Discovery / Classification.....	19
Figure 14: Current Capabilities in Performance Management.....	20

Tables

Table 1: Top Performers Earn Best-in-Class Status.....	8
Table 2: Best-in-Class PACE Framework for Data Loss Prevention	9
Table 3: Competitive Framework for Data Loss Prevention	13
Table 4: PACE Framework Key.....	25
Table 5: Competitive Framework Key.....	25
Table 6: Relationship Between PACE and the Competitive Framework	25

Chapter One: Benchmarking the Best-in-Class

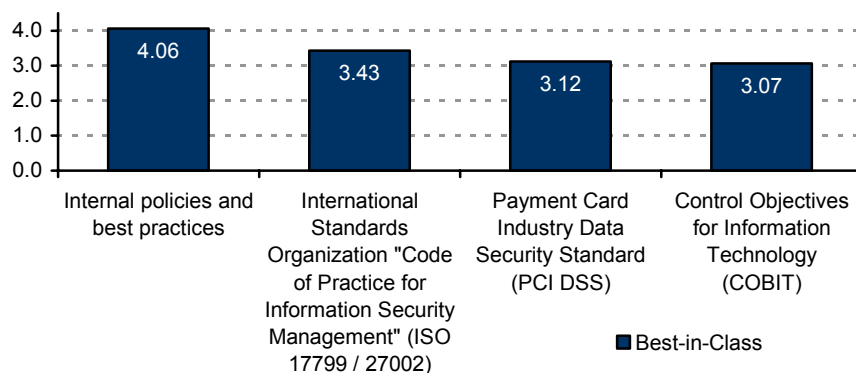
Business Context: Data, Data Everywhere

We are awash in an ocean of information. About 70% of organizations participating in this study indicated a year-over-year increase in the volume of data they generate and attempt to manage, including structured data (e.g., in databases), unstructured data (e.g., in file systems), and semi-structured data (e.g., in e-mail). Little differentiation existed between maturity classes in this regard; the rising tide of information is truly lifting all boats.

In Aberdeen's *Encryption and Key Management* benchmark report (August 2007), the traditional, perimeter-based approach to protecting sensitive data was noted as becoming increasingly impractical and ineffective as more open, flexible network access and distributed computing models dissolve the network perimeter. In its place, an **information-centric** approach to protecting sensitive data is clearly emerging. In this context, data loss prevention ("DLP") solutions are best seen as important elements of an overall strategy to identify, classify, protect, and manage information as part of such an information-centric approach.

In the current study, it was clear that the organizations with top performance in preventing data loss were more proactive and purposeful in their investments, as opposed to making purely reactive investments in the wake of actual data security incidents. For example, Figure 1 shows the relatively high impact of internal policies and best practices, industry standards such as PCI DSS, and industry frameworks such as ISO 27002 and COBIT on incremental investments in DLP solutions by Best-in-Class organizations. This indicates that investments by the top performers are being made based on foundational industry standards and frameworks, not on the latest industry hype.

Figure 1: Standards and Best Practices with Highest Impact on Incremental Investments in DLP (1 = Lowest, 5 = Highest)



Source: Aberdeen Group, May 2008

Fast Facts

Percentage of all respondents reporting a year-over-year increase in the volume of:

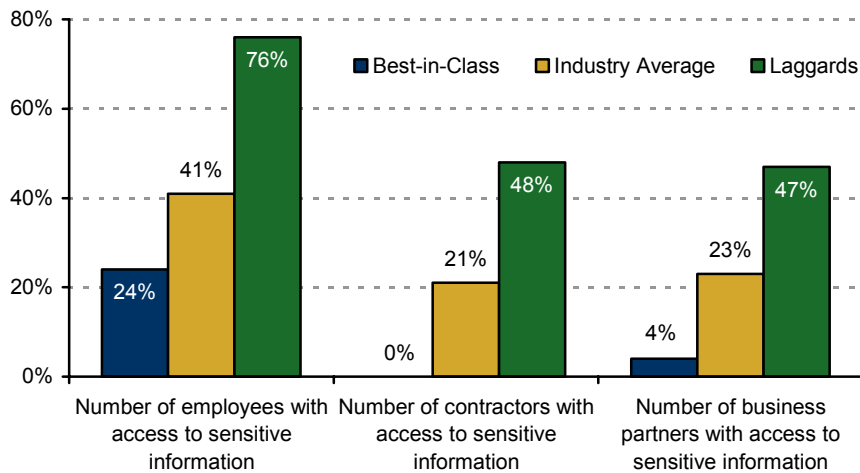
- √ Structured data (e.g., in databases) – 73%
- √ Unstructured data (e.g., in file systems) – 73%
- √ Semi-structured data (e.g., in e-mail) – 68%

Current assessment of risk, based on type of data (scale 1=lowest, 5=highest):

- √ Structured data – 3.46
- √ Unstructured data – 3.14
- √ Semi-structured data – 2.65

In addition, the current study shows that top-performing organizations run a much tighter ship than their counterparts with respect to managing the expansion of access to their sensitive business information. Figure 2 shows the percentage of companies reporting a year-over-year increase in the number of users with access to sensitive information, broken down by the categories of employees, contractors, and business partners. Note, for example, that Best-in-Class organizations were 3-times less likely than Laggards to have increased the number of employees with access to sensitive information, and 12-times less likely with regard to business partners. This is, perhaps, a legacy of the "deny by default and allow by exception" philosophy that is often used to describe the traditional perimeter-based approach to protecting data.

Figure 2: Managing Expansion of Access to Sensitive Information
(% of companies reporting year-over-year increase)



Source: Aberdeen Group, May 2008

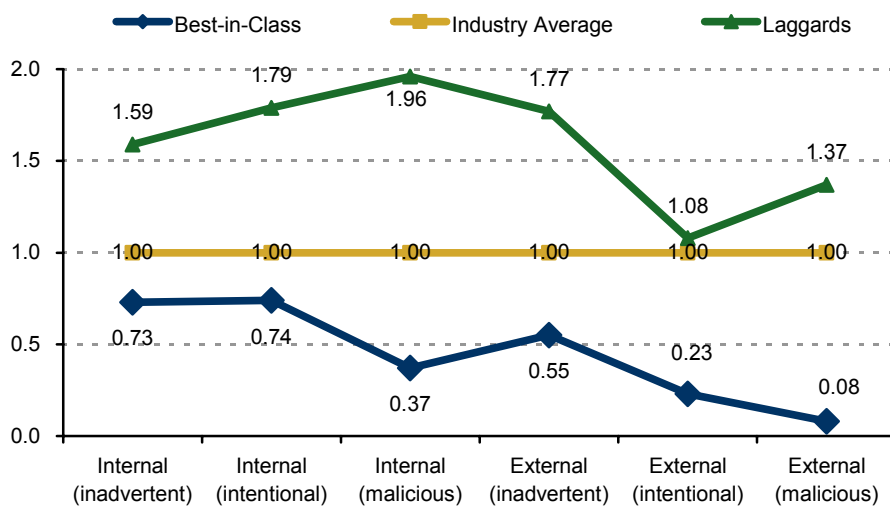
No matter how restrictive or permissive an organization's access policy may be with respect to number of users, however, the risk of data loss comes from all types of data, from innumerable "channels" for potential leakage, and from distinct types of end-user behavior. Across all respondents, the average assessment of the risk of data loss was lowest for semi-structured data (e.g., in e-mail), with risk from unstructured data (e.g., in file systems) assessed at 18% higher and risk from structured data (e.g., in databases) assessed at 31% higher. Other key findings, however (see Table 3), indicate that these high-level assessments of risk are currently based as much on *intuition* as from a systematic discovery and classification of information and a clear mapping of risks and security controls to relevant regulations, standards, and best practices.

In terms of the many possible channels for data leakage, the research shows that the areas perceived as highest risk tend to be related to the endpoints, or to the behavior of the end-users at the endpoints. These include: laptop

loss or theft; e-mail; USB drives and other USB devices; wireless access points; local CD / DVD drives; malicious software (e.g., key loggers); mobile devices (e.g., PDAs, smart phones); Web channels (including webmail, blogs and wikis); and Instant Messaging. Organizations with top performance use a combination of network-based and endpoint-based approaches to prevent data loss, as discussed in more detail in the Technologies section of Chapter Two.

Aberdeen looked at three distinct types of behavior leading to potential data loss incidents – inadvertent, intentional, and malicious – for both internal and external users. The research showed that Best-in-Class organizations assessed the risk of **inadvertent disclosures from trusted insiders** as greater than that of a malicious breach from an external source. This aligns well with the actual number of data loss incidents they reported, as illustrated in Figure 3. The chart shows the number of data loss incidents experienced in the last 12 months, indexed to the Industry Average as 1.0. In this case an index of less than 1.0 is better than the average, while an index greater than 1.0 is worse. In the case of inadvertent disclosures by internal users, for example, Best-in-Class organizations experienced just 27% fewer data loss incidents than the Industry Average – compared to 92% fewer data loss incidents attributed to malicious outsiders. In general, the research shows that while the top performers have achieved significantly better performance at protecting against malicious data loss incidents, their greatest challenge remains in preventing data loss caused by simple human error (inadvertent) and by well-meaning employees trying to carry out their jobs (intentional).

Figure 3: Data Loss Incidents in the Last 12 Months, by Type (indexed to Industry Average = 1.0)



Source: Aberdeen Group, May 2008

Aberdeen's Maturity Class Framework

To distinguish Best-in-Class companies from Industry Average and Laggard organizations, Aberdeen used the year-over-year changes in the following performance criteria:

- Number of data loss incidents
- Number of non-compliance incidents (e.g., failed audits) related to data protection
- Amount of human error related to data protection
- Number of help desk calls related to data protection

Companies with top performance based on these criteria earned Best-in-Class status, as described in Table I. (For additional details on the Aberdeen Maturity Class Framework, see Table 5 in Appendix A.)

Table I: Top Performers Earn Best-in-Class Status

Definition of Maturity Class	Mean Class Performance
<p>Best-in-Class: Top 20% of aggregate performance scorers</p>	<ul style="list-style-type: none"> ▪ 37% decreased the number of actual data loss incidents over the last 12 months ▪ 51% decreased the number of non-compliance incidents (e.g., failed audits) related to data protection over the last 12 months ▪ 40% decreased the amount of human error related to data protection over the last 12 months ▪ 36% decreased the number of help desk calls related to data protection over the last 12 months
<p>Industry Average: Middle 50% of aggregate performance scorers</p>	<ul style="list-style-type: none"> ▪ 2% increased the number of actual data loss incidents over the last 12 months ▪ 4% increased the number of non-compliance incidents (e.g., failed audits) related to data protection over the last 12 months ▪ 4% increased the amount of human error related to data protection over the last 12 months ▪ 8% increased the number of help desk calls related to data protection over the last 12 months
<p>Laggard: Bottom 30% of aggregate performance scorers</p>	<ul style="list-style-type: none"> ▪ 59% increased the number of actual data loss incidents over the last 12 months ▪ 32% increased the number of non-compliance incidents (e.g., failed audits) related to data protection over the last 12 months ▪ 63% increased the amount of human error related to data protection over the last 12 months ▪ 62% increased the number of help desk calls related to data protection over the last 12 months

Source: Aberdeen Group, May 2008

Best-in-Class PACE Model

Using DLP and complementary data protection solutions to prevent data loss requires a combination of strategic actions, organizational capabilities, and enabling technologies – referred to by Aberdeen as the Best-in-Class PACE Framework (for a description of the Aberdeen PACE Framework, see Table 4 in Appendix A). The characteristics exhibited by Best-in-Class organizations in this study are summarized in Table 2.

Table 2: Best-in-Class PACE Framework for Data Loss Prevention

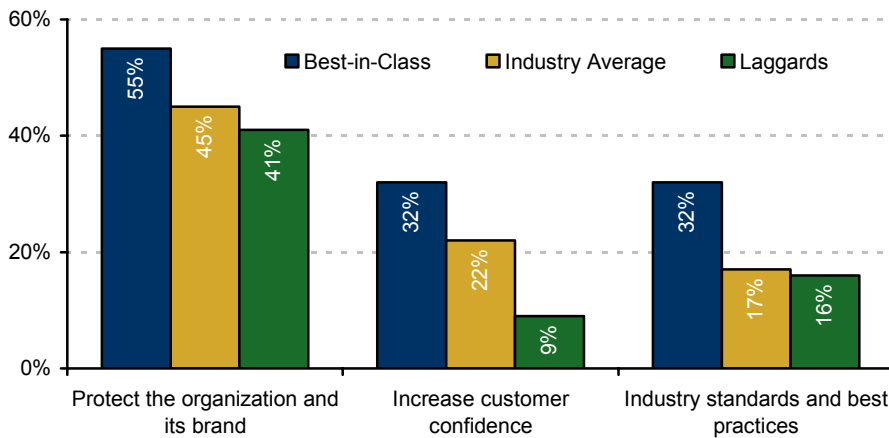
Pressures	Actions	Capabilities	Enablers
<ul style="list-style-type: none"> ▪ Protect the organization and its brand 	<ul style="list-style-type: none"> ▪ Establish and enforce consistent policies and procedures for data protection ▪ Protect data at rest (or "in use") on endpoint systems ▪ Educate end-users about data protection policies and best practices ▪ Protect data at rest in back-end systems (e.g., storage/backup systems, databases, applications) ▪ Monitor for the transmission of sensitive data (real-time) 	<ul style="list-style-type: none"> ▪ Discovery of all information assets ▪ Classification of information assets ▪ Consistent policies for data at rest, data in motion, and data "in use" at the endpoints ▪ Responsible executive or team with primary ownership for data protection ▪ Formal documentation, awareness and end-user training programs around data protection ▪ Real-time notification of policy violations ▪ User-based enforcement of data protection policies ▪ Automated enforcement of data protection policies 	<ul style="list-style-type: none"> ▪ Web monitoring and filtering ▪ Web application firewall ▪ E-mail monitoring and filtering ▪ Database activity monitoring ▪ Network-based DLP monitoring ▪ Agent-based DLP monitoring ▪ File / folder encryption ▪ Network encryption ▪ Backup / Archive encryption ▪ Storage encryption ▪ Database encryption ▪ Full-disk encryption ▪ E-mail encryption ▪ USB drive encryption ▪ Information discovery tools ▪ Information classification tools ▪ Endpoint port controls

Source: Aberdeen Group, May 2008

Best-in-Class Strategies

Consistent with the general trends seen in Aberdeen's research over the past several months, "protect the organization and its brand" was a dominant pressure driving current investments in data loss prevention by Best-in-Class organizations (Figure 4). "Increase customer confidence" and "industry standards and best practices" round out the leading business drivers identified in this study.

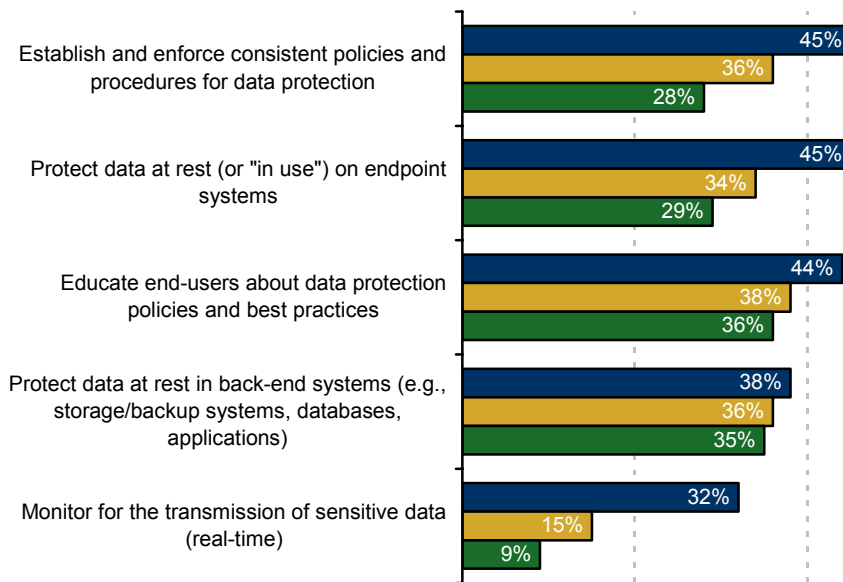
Figure 4: Top Pressures Driving Current Investments in DLP



Source: Aberdeen Group, May 2008

Figure 5 illustrates the leading strategies that are driving current investments in DLP. Not surprisingly, "establish and enforce consistent policies" is at the top of the list. Closely related is "educate end-users about data protection policies and best practices". Establishing consistent policies and making end-users aware of them is necessary, but not sufficient, for top performance. As shown in Figure 5, Best-in-Class organizations are also more likely to have explicit strategies to protect their data wherever it flows: to the endpoints, in back-end systems, and in transit.

Figure 5: Leading Strategies Driving Current Investments in DLP



Source: Aberdeen Group, May 2008

Best-in-Class organizations in this study were determined by their year-over-year improvements in security and compliance, and by their year-over-year improvements in key elements of cost (i.e., human error, help desk calls) related to preventing data loss. In the next chapter, we will see what the top performers are doing to achieve these gains.

Aberdeen Insights – Strategy

Most likely, your organization's "information footprint" is much larger – and growing much faster – than anyone would have predicted just a few short years ago. Many security practitioners tasked with preventing data loss feel stuck between the equivalent of *Scylla* and *Charybdis*, the twin perils of Greek mythology – on the one hand, the insatiable sea monster of more data, more flexible network access, and ever-higher end-user expectations; and on the other hand, the whirlpool of greater security threats and more stringent compliance requirements that sucks in large quantities of precious IT resources. As in *The Odyssey*, we are sometimes forced to choose which monster to confront in order to pass as safely as possible through the narrow straight.

Aberdeen's research on data loss prevention confirms that the risk of data loss comes from all types of data, from innumerable "channels" for potential leakage, and from end-user behavior ranging from inadvertent, to well-intentioned, to malicious. Unfortunately, strategies that focus on protecting against data loss in only one channel do not solve the overall problem; little leaks can sink the ship. In an information-centric approach to protecting sensitive data, organizations with top performance use a combination of network-based and agent-based (i.e., endpoint-based) solutions to prevent data loss, and buyers should consider solutions that allow them to protect sensitive data wherever it flows: at rest in back-end systems, in motion on the network, and in use at the endpoints. In this context, DLP solutions are best seen as important elements of an overall strategy to identify, classify, protect, and manage sensitive information as part of such an information-centric approach.

"We view DLP solutions as highly complementary to encryption. Ideally, we would like to be able to encrypt automatically, by policy, based on the content. At the same time, however, we still believe that we need to communicate exactly what's going on to our users. Because in the long run, we actually want to change user behavior."

~ CISO,
mid-size high-tech company

Chapter Two: Benchmarking Requirements for Success

Strategies to prevent data loss ultimately lead to the selection of one or more specific solutions for identifying, classifying, protecting and / or managing sensitive information. These choices – along with the policy, planning, process, and organizational elements of implementation – are critical success factors in the ability to realize the business benefits of better security, sustained compliance, reduced human error and reduced help desk calls related to data protection.

Fast Facts

√ Across all respondents, the average number of data loss incidents (inadvertent, intentional, and malicious) over the last 12 months ranged **between 2 and 5**

Case Study – Gaming and Entertainment Complex, Northeastern United States

Gaming and entertainment is big business. Upon the successful completion of a multi-year expansion project over the next two years, one gaming and entertainment complex headquartered in the Northeastern United States is expected to offer approximately 7,000 slot machines, 380 table games, 2,100 hotel rooms, 75 restaurants and retail outlets, 30 bars and lounges, and 4 entertainment venues. The business generated >\$1.7B in annual revenue in 2007, supported by 10,000 total employees, including approximately 3,000 knowledge workers.

It projects a high-rolling image, but the business is actually based on highly conservative management of risk. Within this culture, the organization's Manager of Security Risk has taken a deliberate, systematic approach to rolling out solutions designed to protect the infrastructure and prevent data loss. "I wanted to detect non-compliance with established policies. I wanted to detect non-managed devices. And most importantly, I wanted to protect against the inadvertent disclosure of sensitive customer data."

Solutions which have been deployed to date include:

- Proactive scanning of the endpoints to prevent malware, spyware and other unwanted programs from being installed and infecting the systems.
- Enforcement of compliance with policy at the network access points, to prevent non-compliant systems from gaining access to the network.
- Encryption at the endpoints, to protect sensitive data on desktops, laptops, portable media, and other mobile devices.
- Scanning of inbound and outbound e-mails for spam, viruses, and inappropriate content.

Expansion of monitoring and filtering class solutions, both network-based and endpoint-based, is also under consideration. "The vast majority of issues related to protecting data are inadvertent, not malicious. But if we can effectively detect them, we can shut them down."

Competitive Assessment

Aberdeen analyzed the aggregated metrics of surveyed companies to determine whether their performance ranked as Best-in-Class, Industry Average, or Laggard. In addition to having common performance levels, each class also shared characteristics in five important categories: (1) **process** (the approaches taken to execute daily operations); (2) **organization** (corporate focus and collaboration among stakeholders); (3) **knowledge management** (putting data in context and exposing it to relevant stakeholders); (4) **technology** (the selection of appropriate tools, and the effective deployment of those tools); and (5) **performance management** (the ability of the organization to measure results to improve the business). These characteristics, identified in Table 3, serve as a guideline for best practices, and correlate directly with Best-in-Class performance across the associated metrics.

Table 3: Competitive Framework for Data Loss Prevention

	Best-in-Class	Average	Laggards
Process	Consistent policies for data at rest (back-end systems)		
	64%	39%	32%
	Consistent policies for data in motion		
	73%	34%	31%
	Consistent policies for data at rest (or "in use") at the endpoints		
	64%	45%	37%
Organization	Systematic implementation / rollout processes for data protection solutions		
	68%	25%	19%
	Responsible executive or team with primary ownership for data protection		
Knowledge	77%	60%	55%
	Formal documentation, awareness and end-user training programs around data protection		
Technology	59%	34%	27%
	Discovery of all information assets		
	50%	34%	27%
Technology	Classification of information assets		
	59%	36%	32%
Technology	Automated creation of policies based on discovery and classification of information		
	36%	12%	3%

	Best-in-Class	Average	Laggards
	Automated enforcement of data protection policies (unaided by end-users)		
	64%	10%	6%
	Automated enforcement of policies (with real-time alerts and notifications to end-users)		
	48%	16%	10%
	Current use of data protection technologies: see Figure 11, Figure 12, and Figure 13		
Performance	Effective measurement of information required for governance of data protection initiatives:		
	<ul style="list-style-type: none"> ▪ Number of data loss incidents 68% ▪ Source (channels) of data loss incidents 68% ▪ Source (users) of data loss incidents 73% ▪ Financial impact of data loss incidents 55% ▪ Total costs associated with protecting data 45% 	<ul style="list-style-type: none"> ▪ Number of data loss incidents 31% ▪ Source (channels) of data loss incidents 34% ▪ Source (users) of data loss incidents 34% ▪ Financial impact of data loss incidents 24% ▪ Total costs associated with protecting data 15% 	<ul style="list-style-type: none"> ▪ Number of data loss incidents 31% ▪ Source (channels) of data loss incidents 26% ▪ Source (users) of data loss incidents 25% ▪ Financial impact of data loss incidents 19% ▪ Total costs associated with protecting data 6%

Source: Aberdeen Group, May 2008

Capabilities and Enablers

Based on the comparisons within the Competitive Framework and interviews with select respondents, analysis of the Best-in-Class highlights the degree to which they have developed their data loss prevention business processes beyond those of their Industry Average and Laggard counterparts.

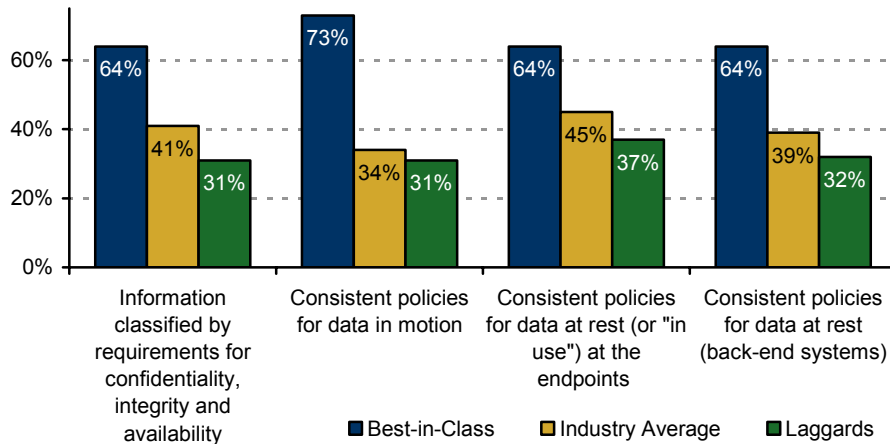
Process

Identification and classification of data is the foundation for consistent data protection policies. "You can't protect what you can't manage," says one VP, "And you can't manage what you can't see." Moreover, Best-in-Class companies have established consistent policies for data wherever it goes: in back-end systems, in flight, and at the endpoints (Figure 6). Solutions providers who support these capabilities lay out a more straightforward path to Best-in-Class performance.

"When it comes to preventing data loss, there is a wide spectrum of degrees of pain that you can inflict on your end-user populations. In our environment, we can't get away with imposing burdens on the end-users."

~ Member of IT Staff,
higher education

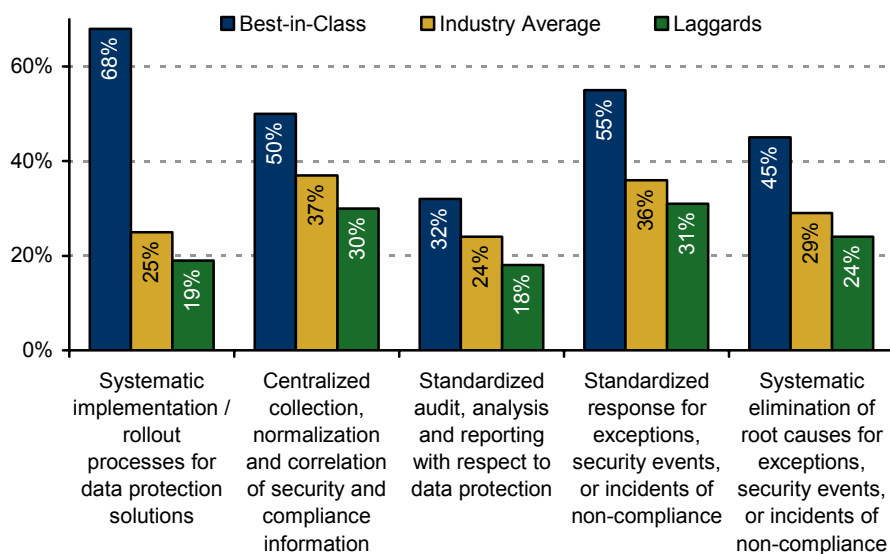
Figure 6: Classification is the Foundation for Consistent Policies



Source: Aberdeen Group, May 2008

In addition, Best-in-Class organizations have implemented systematic implementation and rollout processes for their data protection solutions (Figure 7). They are more likely to centralize the collection of security and compliance information, with standardized audit, analysis and reporting capabilities. When data loss incidents do occur, they also have more standardized incident response, and systematic elimination of root causes to prevent future incidents. All of this underscores the more proactive and purposeful approach to preventing data loss taken by the Best-in-Class companies, relative to the other maturity classes.

Figure 7: Systematic Rollout and Proactive Management

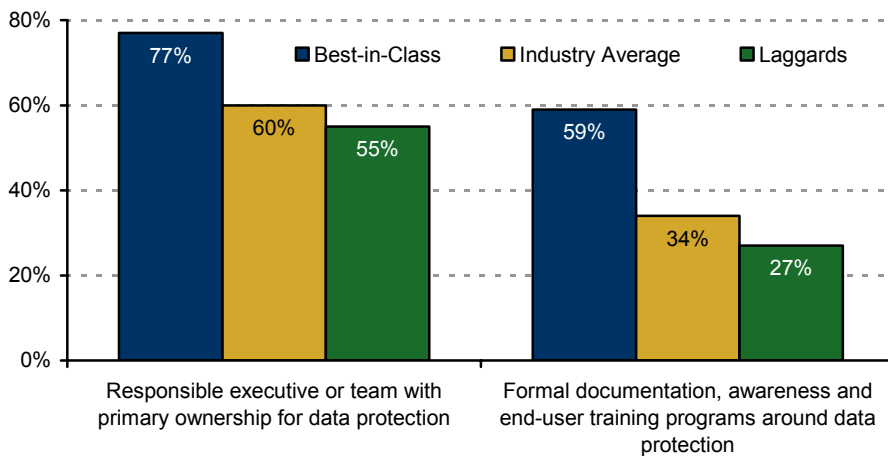


Source: Aberdeen Group, May 2008

Organization

Aberdeen's research has demonstrated time and time again that Best-in-Class organizations have established responsible leaders for their information security initiatives – i.e., “the one throat to choke” principle. The same is true for preventing data loss. In addition, the Best-in-Class do a significantly better job (more than 2-times more than Laggards) at educating end-users on their data protection policies (Figure 8). Given the much higher frequency of inadvertent and well-intentioned data leakage incidents by trusted insiders, investments in end-user awareness and education should provide positive returns.

Figure 8: One Throat to Choke; Educated End-Users

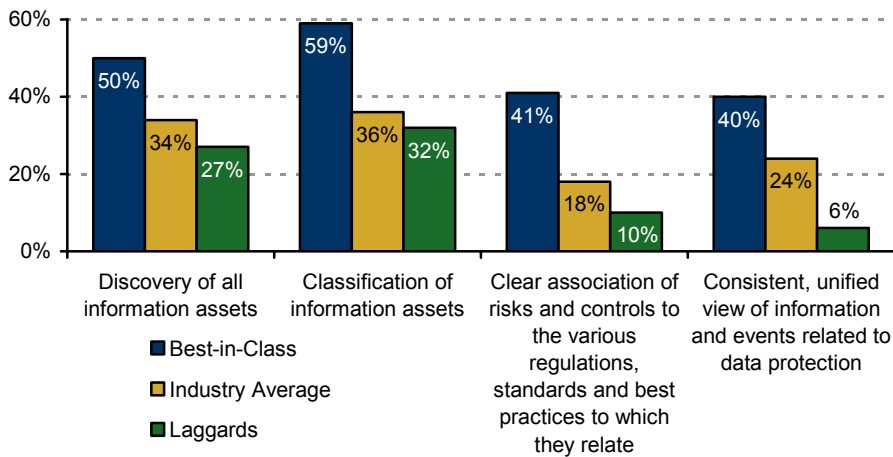


Source: Aberdeen Group, May 2008

Knowledge Management

As noted, identification and classification of data is the foundation for consistent data protection policies. Figure 9 illustrates that Best-in-Class organizations do in fact identify/discover and classify their information to a higher degree than their counterparts, although at less than 60% there is still considerable room for improvement. In addition, they are 2-times more likely than the Industry Average and 4-times more likely than Laggards to map risks and security controls to the relevant set of regulations, standards, and best practices. In other words, with respect to policies for preventing data loss they are more fully aware of not only the "what", but also the "why".

Figure 9: Visibility into Key Data and Intelligence

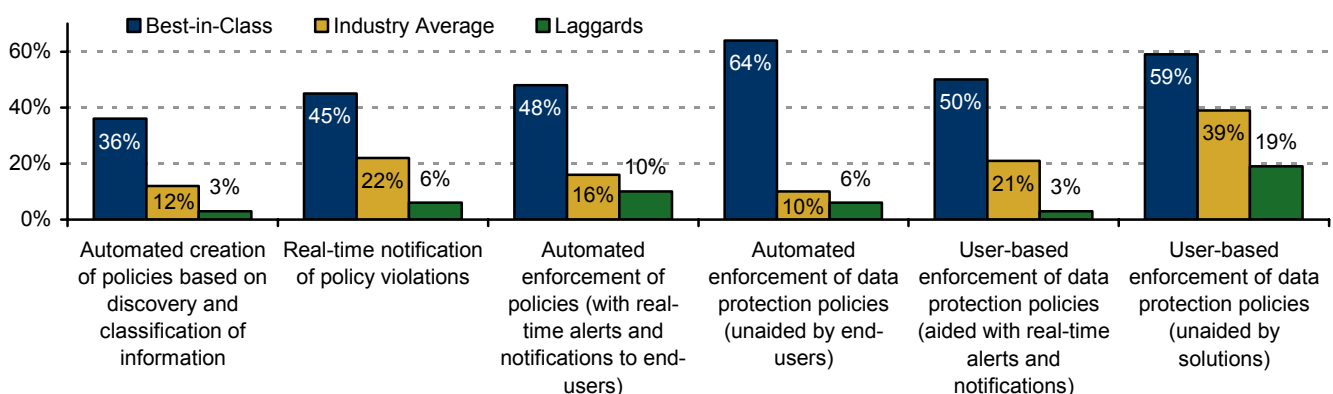


Source: Aberdeen Group, May 2008

Technology

The automated creation of policies based on discovery / classification is a newly emerging capability, as shown in Figure 10. Just 36% of Best-in-Class organizations report this as a current capability, although this is in fact 3-times higher than the Industry Average. The research shows that current practice with respect to enforcement of policies is a mixture of both automatic and user-based, and a mixture of both aided and unaided by real-time alerts and notifications from the DLP solutions. Anecdotal evidence from direct discussions with end-users indicates a wide spread of opinion on these matters. Some feel that end-users should be proactively involved, with an eye towards changing behavior in the long term; others feel that depending on end-user behavior for any aspect of information security leads to certain failure. Aberdeen will continue to explore these issues in its future research.

Figure 10: Many Approaches to Automated Enforcement of Data Protection Policies



Source: Aberdeen Group, May 2008

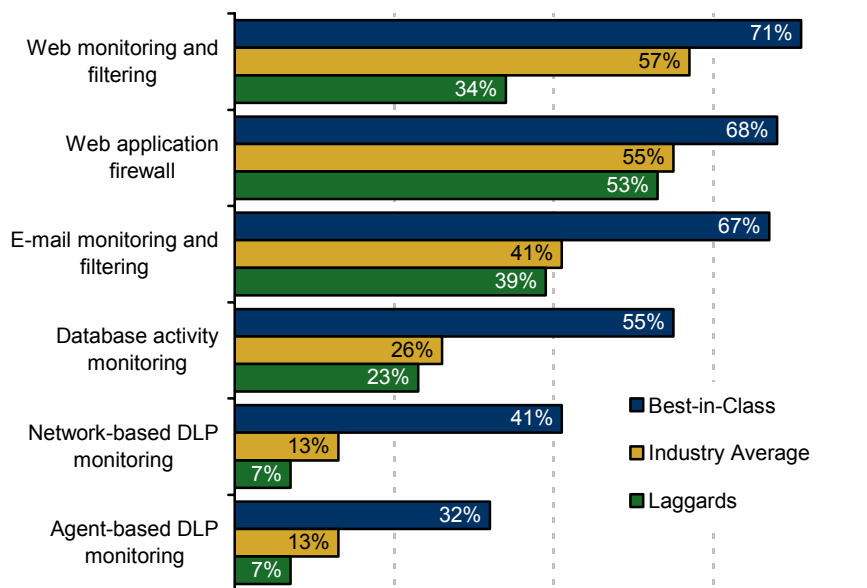
The current study also revealed that the Best-in-Class are most likely to automate "passive" actions related to preventing data loss, such as *detect, alert, log, notify, monitor* and *report*. They are next most likely to automate coarse-grained controls, e.g., *block, encrypt, and quarantine*. Least likely to be automated are controls over more granular actions – e.g., *move, save, copy, delete, print, burn* – although the Best-in-Class are still more likely to implement these than their Industry Average and Laggard counterparts. Overall, the data speaks to a pragmatic "Crawl / Walk / Run" approach that begins with automation of the more passive actions, progresses to automation of the more coarse-grained controls, and potentially proceeds to automation of the more granular controls.

"We had very detailed policies, but they had no teeth in terms of enforcement. Our first big political challenge was to decide who gets notified in the case of a policy violation: Security? The end-user? His manager? Or simply the logs? The technology was the easy part. We're still learning how to make the people and process parts work for us."

~ IT Director,
mid-size enterprise

Current use of enabling technologies demonstrates that Web monitoring and filtering, e-mail monitoring and filtering, and database monitoring and filtering are well-established (Figure 11). Between 55% and 71% of Best-in-Class organizations have currently deployed these solutions. DLP monitoring (whether network- or agent-based) is newer and relatively lower in current use, with about a third of top performers indicating current deployments. Still, deployment of DLP is clearly a distinguishing characteristic of the Best-in-Class, by a factor of 2.5-times to 3-times compared to the Industry Average.

Figure 11: Enabling Technologies – Monitoring and Filtering

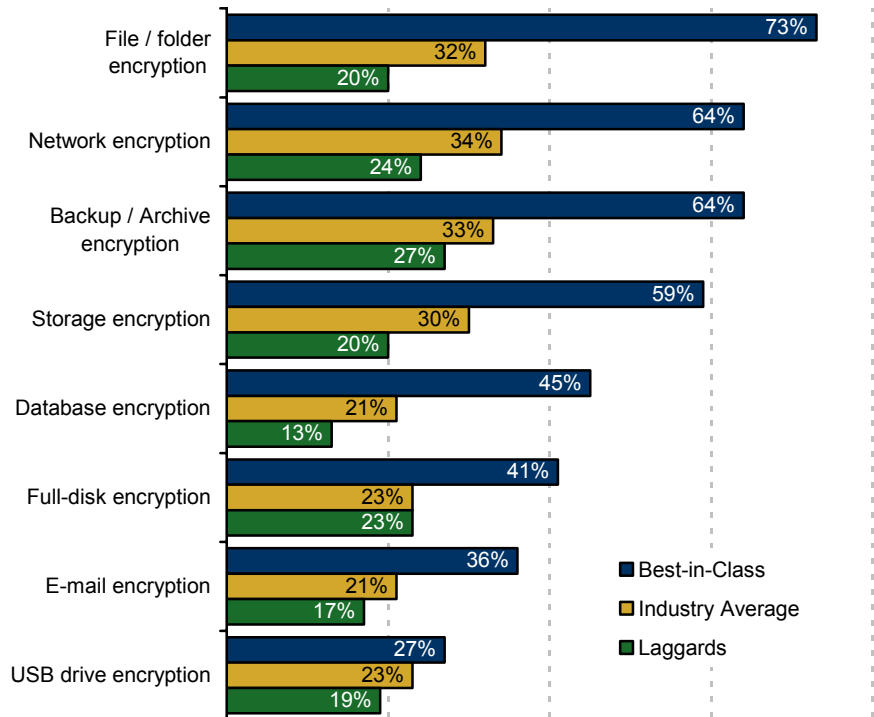


Source: Aberdeen Group, May 2008

Previous Aberdeen research has shown an expanding use of encryption across multiple enterprise use cases – in the back-end, on the network, and at the endpoints – and the current research is consistent with those findings. As shown in Figure 12, the Best-in-Class are more likely to have deployed encryption across all surveyed use cases. Strong growth in encryption deployments should continue in all use cases as well, based on

the responses regarding future intent (i.e., planned deployments in the next 12 months, and current evaluations). The highest growth areas indicated for encryption include full-disk, USB drives, e-mail, and file/folder.

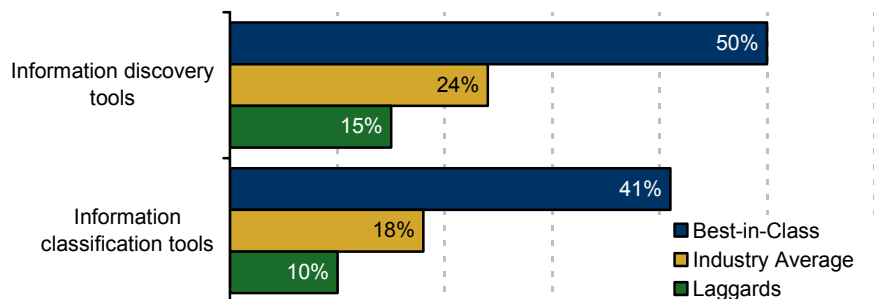
Figure 12: Enabling Technologies – Encryption



Source: Aberdeen Group, May 2008

Finally, top performers are 3-times to 4-times more likely than bottom performers to have deployed automated information discovery and classification tools (Figure 13). For most companies, discovery and classification are starting point for successful deployment of DLP solutions, and the first steps on the path towards broader protection of data.

Figure 13: Enabling Technologies – Discovery / Classification

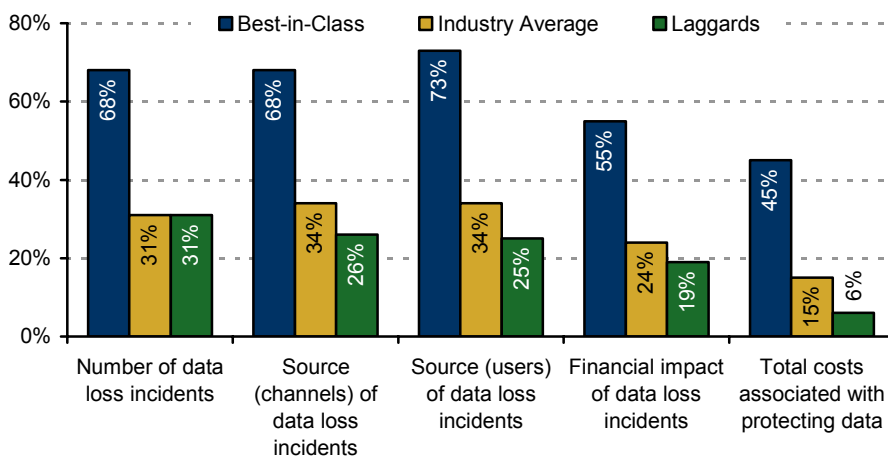


Source: Aberdeen Group, May 2008

Performance Management

Effective governance of data protection initiatives requires effective measurement of key performance indicators. Figure 14 illustrates that Best-in-Class companies are better able to measure the number of data loss incidents, the source (both channels, and users) for data leakage, the financial impact of data loss incidents, and the total costs associated with protecting data. Once again, this points to a more disciplined and planful approach to preventing data loss by organizations achieving top performance.

Figure 14: Current Capabilities in Performance Management



Source: Aberdeen Group, May 2008

Aberdeen Insights – Technology

The risk of data loss cannot be isolated to one type of data, one channel for leakage, or one mode of end-user behavior. The most effective strategies for preventing data loss will include a combination of enabling technologies, including:

- Data discovery and classification
- Data monitoring and filtering – including web, e-mail, database, and network-based DLP
- Endpoint data protection – including agent-based DLP, encryption, and endpoint port controls

In this context, DLP solutions are best seen as important elements of an overall strategy to identify, classify, protect, and manage sensitive information as part of an information-centric approach. Starting from their traditional positions of strength, most solution providers have

continued

Aberdeen Insights – Technology

begun to extend their offerings (through acquisition, partnerships, or organic development) to address this more comprehensive approach to preventing data loss.

Discovery, classification, and establishment of consistent policies for data at rest in the back-end, data in flight on the network, and data in use at the endpoints should be assumed as table stakes for any data loss prevention initiative. From there, the research indicates that best practice with respect to the automated enforcement of data protection policies follows a pragmatic "Crawl / Walk / Run" approach:

- Automate "passive" actions related to preventing data loss, such as *detect, alert, log, notify, monitor* and *report*. Use this information to establish a baseline, fine-tune policies, and educate the organization (both end-users and management).
- Automate coarse-grained controls, e.g., *block, encrypt, and quarantine*. Most data leakage which is either inadvertent or attributable to well-intentioned insiders will be addressed by this phase.
- Consider automated controls over more granular actions on data, e.g., *move, save, copy, delete, print, burn*. These functions may almost be viewed as a sort of "poor man's Enterprise Rights Management", and are much less widely implemented than the passive actions and coarse-grained controls outline above.

Chapter Three: Recommended Actions

Whether a company is trying to move its performance in data loss prevention from Laggard to Industry Average, or Industry Average to Best-in-Class, the following actions will help spur the necessary performance improvements.

Laggard Steps to Success

- **Discover and Classify the Data.** Less than one-third of Laggards reported that they have identified and classified their information assets. You can't protect what you don't manage, and you can't manage what you can't see.
- **Establish Consistent Policies.** Between 31% and 37% of Laggard organizations indicated that they have consistent policies for data at rest, data in motion, and data at the endpoints. Based on the discovery / classification process and a clear understanding of risk, establishing consistent policies for protecting sensitive data should be much easier than starting from a blank page.
- **Educate the Users.** Just 27% of Laggards currently have formal documentation, awareness and education programs around data protection. Since a high percentage of data loss incidents stem from trusted insiders, making users fully aware of their responsibilities for protecting the company's sensitive data should be a given.

Industry Average Steps to Success

- **Discover and Classify the Data.** The Industry Average were only slightly better than Laggards in this regard; slightly more than one-third reported that they have identified and classified their information assets.
- **Establish Consistent Policies.** Between 34% and 45% of Industry Average organizations indicated that they have consistent policies for data at rest, data in motion, and data at the endpoints. These firms should leverage the discovery / classification process and establish consistent policies based on a risk-based approach (e.g., as a function of potential data loss incidents and their probabilities of occurrence).
- **Educate the Users.** Just 34% of the Industry Average currently have formal documentation, awareness and education programs around data protection. End users should be made fully aware of their responsibilities for protecting the organization's sensitive data.
- **Roll Out Data Protection Solutions.** Only 25% of the Industry Average indicated they have systematic implementation processes for data protection solutions, compared to 68% of the Best-in-Class.

Fast Facts

Percentage of respondents currently implementing endpoint port controls:

√ 32% Best-in-Class

√ 20% Industry Average

√ 10% Laggards

"The message to users is this: 'You have no privacy. We're going to monitor every piece of information that comes in and out of the computer that was issued to you.' Just how this message is packaged and delivered to end-users, however, is critical."

~ CISO, global enterprise

Up-front investments in planning will help to ensure a smoother rollout and to maximize end-user acceptance.

Best-in-Class Steps to Success

- **Discover and Classify the Data.** Just 50% of the Best-in-Class reported that they have identified and classified all information assets. This is the foundation for establishing consistent policies for data at rest in the back-end, data in flight on the network, and data in use at the endpoints.
- **Educate the Users.** Nearly 3 out of 5 of the Best-in-Class currently have formal documentation, awareness and education programs around data protection, about 74% higher than the Industry Average. Automating "passive" actions related to preventing data loss, such as *detect, alert, log, notify, monitor* and *report*, can also be used to establish a baseline, fine-tune policies, and educate the organization.
- **Automate Enforcement.** Just under two-thirds of Best-in-Class organizations automate enforcement of their data protection policies with no aid from end-users. Automation of coarse-grained controls, e.g., *block, encrypt, and quarantine* would address most inadvertent or well-intentioned data leakage incidents by trusted insiders.

Aberdeen Insights – Summary

DLP solutions are important elements of an overall strategy to identify, classify, protect, and manage sensitive information. Based on planned deployments in the next 12 months and current evaluations, the research indicates strong growth for both network-based DLP and agent-based (i.e., endpoint-based) DLP over the next 12 months. No material shift between network-based and agent-based DLP is indicated by the research data.

There is a discernable shift towards actively protecting data associated with the endpoints, however, which includes not only DLP but also endpoint-oriented encryption (e.g., file/folder, full-disk, e-mail, and USB drives) and endpoint port controls. The highly complementary nature of these solutions is further evidenced through the evolving solution portfolios of leading vendors. Starting from their traditional positions of strength, most solution providers have begun to extend their offerings (through acquisition, partnerships, or organic development) to address a more comprehensive approach to preventing data loss. This trend should be helpful to organizations of all maturity classes, as it promises to reduce the software footprint at the endpoints and to simplify the burden of management, audit, analysis and reporting.

Send to a Friend 

Appendix A: Research Methodology

Between April and May 2008, Aberdeen examined the range of approaches currently being taken to protect against the loss or exposure of sensitive data. The experiences and intentions of approximately 120 organizations from a diverse set of industries are represented in this study. Aberdeen supplemented this online survey effort with interviews with select survey respondents, gathering additional information on data loss prevention strategies, experiences, and results.

Responding organizations had the following demographics:

- *Job title / function:* The research sample included respondents with the following job titles: C-level (16%); Vice President / General Manager (12%); Director (14%); Manager (14%); Staff / Consultant (35%); and Other (9%). The largest segment by functional responsibility was IT, representing 46% of the sample.
- *Industry:* The research sample included respondents from a wide range of industries. The largest segments were financial (15%) and government / defense (9%).
- *Geography:* A majority of respondents (59%) were from the Americas. Remaining respondents were from the Asia-Pacific region (12%) and Europe / Middle East / Africa (29%).
- *Company size:* Twenty-two percent (22%) of respondents were from large enterprises (annual revenues above US \$1 billion); 18% were from midsize enterprises (annual revenues between \$50 million and \$1 billion); and 60% of respondents were from small businesses (annual revenues of \$50 million or less).

Solution providers recognized as sponsors were solicited after the fact and had no substantive influence on the direction of this report. Their sponsorship has made it possible for Aberdeen Group to make these findings available to readers at no charge

Table 4: PACE Framework Key

Overview
<p>Aberdeen applies a methodology to benchmark research that evaluates the business pressures, actions, capabilities, and enablers (PACE) that indicate corporate behavior in specific business processes. These terms are defined as follows:</p> <p>Pressures — external forces that impact an organization’s market position, competitiveness, or business operations (e.g., economic, political and regulatory, technology, changing customer preferences, competitive)</p> <p>Actions — the strategic approaches that an organization takes in response to industry pressures (e.g., align the corporate business model to leverage industry opportunities, such as product / service strategy, target markets, financial strategy, go-to-market, and sales strategy)</p> <p>Capabilities — the business process competencies required to execute corporate strategy (e.g., skilled people, brand, market positioning, viable products / services, ecosystem partners, financing)</p> <p>Enablers — the key functionality of technology solutions required to support the organization’s enabling business practices (e.g., development platform, applications, network connectivity, user interface, training and support, partner interfaces, data cleansing, and management)</p>

Source: Aberdeen Group, May 2008

Table 5: Competitive Framework Key

Overview	
<p>The Aberdeen Competitive Framework defines enterprises as falling into one of the following three levels of practices and performance:</p> <p>Best-in-Class (20%) — Practices that are the best currently being employed and are significantly superior to the Industry Average, and result in the top industry performance.</p> <p>Industry Average (50%) — Practices that represent the average or norm, and result in average industry performance.</p> <p>Laggards (30%) — Practices that are significantly behind the average of the industry, and result in below average performance.</p>	<p>In the following categories:</p> <p>Process — What is the scope of process standardization? What is the efficiency and effectiveness of this process?</p> <p>Organization — How is your company currently organized to manage and optimize this particular process?</p> <p>Knowledge — What visibility do you have into key data and intelligence required to manage this process?</p> <p>Technology — What level of automation have you used to support this process? How is this automation integrated and aligned?</p> <p>Performance — What do you measure? How frequently? What’s your actual performance?</p>

Source: Aberdeen Group, May 2008

Table 6: Relationship Between PACE and the Competitive Framework

PACE and the Competitive Framework – How They Interact
<p>Aberdeen research indicates that companies that identify the most influential pressures and take the most transformational and effective actions are most likely to achieve superior performance. The level of competitive performance that a company achieves is strongly determined by the PACE choices that they make and how well they execute those decisions.</p>

Source: Aberdeen Group, May 2008

Appendix B: Related Aberdeen Research

Related Aberdeen research that forms a companion or reference to this report includes:

- [PCI DSS and Protecting Cardholder Data: Year-over-Year Benchmark Update](#); publishing June 2008
- [Automating Encryption Key Management](#); January 2008
- [Protecting Data at the Endpoints](#); December 2007
- [Encryption and Key Management](#); August 2007
- [The Ins and Outs of Email Vulnerability](#); July 2007
- [Protecting Cardholder Data](#); June 2007
- [Thwarting Data Loss](#); May 2007

Information on these and any other Aberdeen publications can be found at www.aberdeen.com.

Author: Derek E. Brink, Vice President and Research Fellow, IT Security,
Derek.Brink@aberdeen.com

Since 1988, Aberdeen's research has been helping corporations worldwide become Best-in-Class. Having benchmarked the performance of more than 644,000 companies, Aberdeen is uniquely positioned to provide organizations with the facts that matter — the facts that enable companies to get ahead and drive results. That's why our research is relied on by more than 2.2 million readers in over 40 countries, 90% of the Fortune 1,000, and 93% of the Technology 500.

As a Harte-Hanks Company, Aberdeen plays a key role of putting content in context for the global direct and targeted marketing company. Aberdeen's analytical and independent view of the "customer optimization" process of Harte-Hanks (Information – Opportunity – Insight – Engagement – Interaction) extends the client value and accentuates the strategic role Harte-Hanks brings to the market. For additional information, visit Aberdeen <http://www.aberdeen.com> or call (617) 723-7890, or to learn more about Harte-Hanks, call (800) 456-9748 or go to <http://www.harte-hanks.com>

This document is the result of primary research performed by Aberdeen Group. Aberdeen Group's methodologies provide for objective fact-based research and represent the best analysis available at the time of publication. Unless otherwise noted, the entire contents of this publication are copyrighted by Aberdeen Group, Inc. and may not be reproduced, distributed, archived, or transmitted in any form or by any means without prior written consent by Aberdeen Group, Inc.

Featured Underwriters

This research report was made possible, in part, with the financial support of our underwriters. These individuals and organizations share Aberdeen's vision of bringing fact-based research to corporations worldwide at little or no cost. Underwriters have no editorial or research rights and the facts and analysis of this report remain an exclusive production and product of Aberdeen Group.



The Security Division of EMC

RSA, The Security Division of EMC, is the premier provider of security solutions for business acceleration, helping the world's leading organizations succeed by solving their most complex and sensitive security challenges. RSA's information-centric approach to security guards the integrity and confidentiality of information throughout its lifecycle – no matter where it moves, who accesses it or how it is used.

RSA offers industry-leading solutions and services in identity assurance & access control, data loss prevention, encryption & key management, compliance & security information management and fraud protection. These bring trust to millions of user identities, the transactions that they perform, and the data that is generated.

For additional information on RSA:

174 Middlesex Turnpike

Bedford, MA 01730

(800) 495-1095

www.rsa.com

sales@rsa.com



Utimaco is a leading global provider of data security solutions, enabling mid-to large-size organizations to safeguard their data assets against intentional or unintentional data loss, and to comply with privacy laws. Utimaco's complete range of data security solutions provide full 360 degree data protection for data at rest, data in motion and data in use. Utimaco offers its customers comprehensive on-site support via a world-wide network of certified partners and subsidiaries.

For additional information on Utimaco:

10 Lincoln Road
Foxboro, MA 02035
(508) 543-1008
www.utimaco.com
info@utimaco.com