



Aberdeen *Group*

[Send to a Friend](#) 

Endpoint Security Strategies Part II

The Endpoint Data Protection Benchmark

December 2006



Executive Summary

Study results reveal that while most organizations realize that unprotected endpoints represent a significant risk to the network, the majority have limited or no visibility to assess the compliance of end users to endpoint and data privacy policies.

Best in Class companies, on the other hand, understand the risk of unprotected endpoints and are taking steps to protect sensitive data in use at the endpoint. All Best in Class companies have high to complete visibility of their end user compliance to endpoint and data privacy policies, and in turn, are seeing a reduction in the number of data loss incidents involving endpoints and end users.

Without successful solution implementation we risk the high probability of loss of clients.
— Director of Risk Management for a Business Process Outsourcing Organization

In today's business landscape, one could argue that if your data isn't dynamically flowing to vendors, customers, and colleagues you are not as competitive as you could be in the marketplace. In a culture where it's increasingly becoming more acceptable to email a colleague a PDF of the company's latest forward-looking statement, and to copy sensitive corporate files to a USB key for use at home, there are significant data security concerns among many of today's high-technology enterprises.

All we have to do is prevent one significant IP loss and the cost of the tool is recovered
— Corporate Security Officer, Automotive Industry, Europe

While companies are trying to address these security concerns, they are also under ever-increasing pressure to comply with regulatory policy around personal and private data. Executives continue to lose sleep over the potential exposure of their company's intellectual property as well. With the enormous amount of data at risk, and the massive number of hands in the pot, how can an organization successfully protect their data?

It's clear that in order to be successful, you have to understand where your sensitive data lives, and through which devices, channels, and applications it travels. You must then make appropriate security decisions based on the content of the data and/or the context of the activity taking place. Finally, you must back up the security decisions and policies that are constructed with the appropriate training for end users, thus enabling them to understand the potential risks and to better handle sensitive data in the future. The leading endpoint data protection solutions offer these capabilities, and more.

This report will explore strategies for protecting data at its point of use — the endpoint. This report will also demonstrate why incorporating endpoint data protection into a comprehensive, multi-layer security strategy gives today's corporations' ammunition against sensitive data loss and misappropriation, and likewise provides a solution for the regulatory compliance issues surrounding the problem.

There are many endpoint problems and many endpoint solutions. I believe in a best-of-breed rather than single-vendor approach.
— Partner, Technology Sales and Marketing Firm

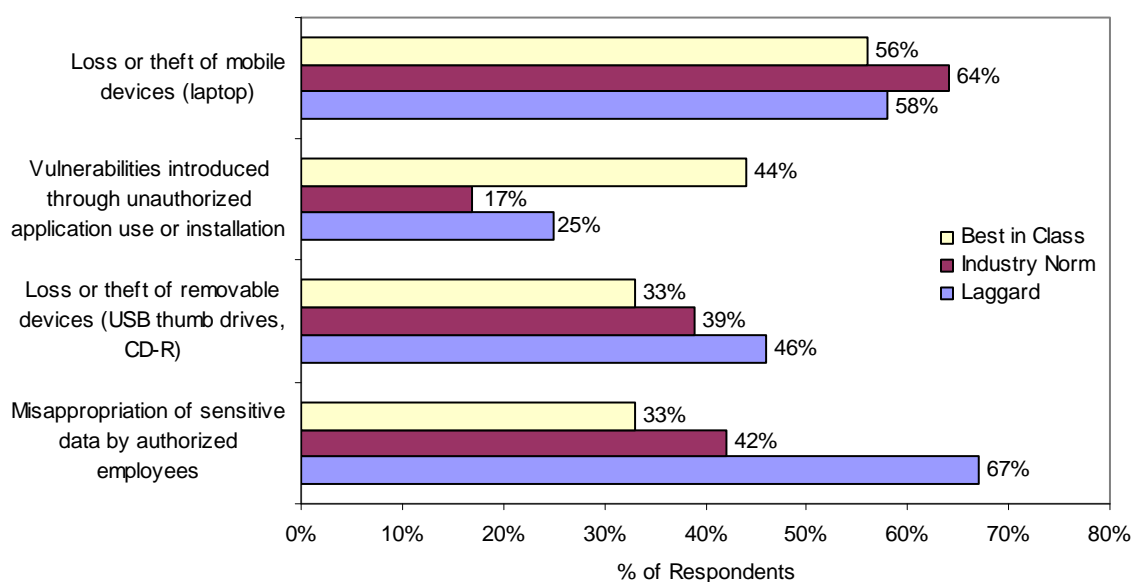
Key Business Value Findings

While approximately two-thirds of surveyed respondents indicate having a strategy to protect data stored and used on endpoints, only 35% feel

their current strategy is adequate. Interestingly, over 85% of the individuals surveyed had little or no visibility into the compliance of end users to endpoint and data privacy policies.

Because of this lack of visibility, organizations are finding it more difficult to institute relevant security policies which will allow them to mitigate some of the risks of doing business in today's high-tech enterprises. Among the top risks influencing our survey respondent's decision regarding endpoint security solutions is loss or theft of mobile devices (such as laptops), vulnerabilities introduced through unauthorized application use or installation, loss or theft of removable devices (such as USB thumb drives, CD-R), and misappropriation of sensitive data by authorized employees (see Figure 1).

Figure 1: The top security risks that influence endpoint security solution decisions



Source: Aberdeen Group, December 2006

Many endpoint data protection solutions in the market today address all or some of these risks through clever implementations of encryption, device/application control, information leak protection, and content analysis.

Our study respondents report there are a number of drivers influencing their decisions to enhance enterprise security, and reduce risk through implementation of an endpoint data protection solution. The majority of respondents (54%) report a desire to implement endpoint data protection in order to limit public exposure of personal or private data. A further 52% of respondents report wanting the solution to protect loss of corporate intellectual property (IP) including product roadmaps, design plans, and financial information. Another 44% of respondents report that they want to protect against the loss of personal or private data.

Interestingly, we found that only 40% of organizations are currently using endpoint data protection technologies, including encryption for data storage, data in transit and infor-



mation leak prevention, to address these security problems. Another 17% are currently assessing or planning to deploy these technologies in the next 12 months.

Implications & Analysis

Companies are having a difficult time achieving end user acceptance and understanding of security requirements when initiating or implementing endpoint data protection solutions. And as a result, enterprises are struggling with a number of risks including sensitive data on lost, stolen, or insecurely disposed of corporate computers/servers; vulnerabilities introduced through unauthorized application use or installation; misappropriation of sensitive data by authorized employees; intellectual property leaks; and regulatory non-compliance.

Organizations can overcome these implementation challenges by improving or creating operational best practices, training staff on regulatory and security requirements, and ensuring deployed systems are automated in their enforcement of endpoint security policies.

Formation of best practices will be a foundation for a successful endpoint data protection implementation. Once drafted, they can be linked back to business goals to ensure the solution meets the needs established on inception. Best practices will also serve as a check and balance measure to establish endpoint compliance to security policy.

Training staff on regulatory and security requirements results in more advantages than just a knowledgeable staff. A well trained staff will be less likely to put your intellectual property or sensitive data in jeopardy. As an added benefit, a staff well trained on security policy will appreciate and take ownership in the process of protecting corporate intellectual property. A number of survey respondents indicated training staff is critical for acceptance and success of the implementation.

Finally, automation can make a successful implementation run on its own. Forty-two percent of our survey respondents report that between 1-5% of IT staff would be dedicated to updating endpoint security policy definitions on an ongoing basis. If any staff is required to maintain the solution, those individuals should be absolutely dedicated to forward looking endpoint data protection policy strategy, not break-fix work. Therefore, it's critical that your endpoint data protection solution is able to automatically enforce endpoint security policy without manual intervention.

If an endpoint data protection solution is successfully implemented, organizations will realize a positive impact on day-to-day operations while also improving their security posture. Seventy percent of respondents either reduced or maintained security staffing requirements, and 22% reported a decrease in the number of data loss incidents involving endpoints or end users in their organizations.

Those organizations that elect to not enforce security policy on their endpoints risk a visible security breach; one that, in the best-case scenario, can generate remediation overhead, and in the worst-case scenario, can expose intellectual property resulting in a

We are very sensitive to the threat of lost or misappropriated data but don't feel that anyone has properly addressed our situation.

— Managing Partner for an IT Consulting Firm

As a matter of fact majority of users liked the knowledge that their information was now secure.

—IS Manager, Health and Beauty Aides Industry

competitive disadvantage, customer loss or regulatory compliance failure. Aberdeen estimates that without a sound endpoint data protection solution in place, ***organizations are at risk of millions of dollars in losses from misplaced intellectual property and unapproved use of valuable, sensitive data.***

Recommendations for Action

Best in Class companies need to review their endpoint data protection plans to ensure that their processes and technologies address not only the loss or theft of endpoints and removable media devices, but also the following: the inadvertent or intentional misappropriation of sensitive data by authorized employees, and unauthorized or improper access of sensitive data by outsiders, employees, and contractors.

In addition to the Best in Class actions, companies should also evaluate their processes to ensure they effectively accomplish the following:

- Create operational procedures and best practices for endpoint data protection
- Put procedures into practice and use the resulting information to generate management reports that support implementing or improving endpoint data protection
- Select systems that provide centralized policy management, comprehensive reporting, and automated policy enforcement
- Train staff to better understand regulatory requirements, security policies, and best practices in support of the endpoint data protection strategy

When evaluating technologies that address risk, organizations should consider endpoint data protection solutions as a requirement to doing business in a safe and responsible manner. Companies should attempt to establish a governance link between business and technology teams to ensure that data at rest is safe, and data in motion is protected throughout its lifecycle.

Our intention is to design the security so people can still work and don't experience security as a shuddering and unexpected halt to their expected way of working.

— Corporate Security Officer, Automotive Industry, Europe

Enforcement of policy must be accomplished in a reliable, non-disruptive manner. Rather than blocking all email attachments, consider an endpoint content inspection solution to determine what should be secured, and follow through with a policy allowing for different levels of encryption based on the content of the attachment. Rather than blocking all copies or moves of data to USB keys, implement a policy which will allow non-business documents to travel freely, but will encrypt or block company confidential documents based on their content. Endpoint

data protection solutions, if properly leveraged, enable companies to better understand their data security issues and to automatically bring themselves into compliance through automated policy enforcement.

[Send to a Friend](#) 

Table of Contents

Executive Summary	ii
Key Business Value Findings.....	ii
Implications & Analysis	iv
Recommendations for Action.....	v
<i>Chapter One: Issue at Hand</i>	4
<i>Chapter Two: Key Business Value Findings</i>	6
Data protection risks areas	6
Why is endpoint data protection so important?	8
Challenges and Responses	9
Solutions.....	12
How to get started.....	14
Strategies for those already using endpoint data protection solutions	17
Solution Satisfaction	19
<i>Chapter Three: Implications & Analysis</i>	22
Process and Organization	23
Technology Use	23
Security Solutions Currently In Use	23
Pressures, Actions, Capabilities, Enablers (PACE).....	24
Business Impact of Endpoint Data Protection Solutions	25
<i>Chapter Four: Recommendations for Action</i>	26
Laggard Steps to Success.....	26
Industry Norm Steps to Success.....	27
Best in Class Next Steps	27
Featured Underwriters.....	Error! Bookmark not defined.
<i>Appendix A: Research Methodology</i>	29
<i>Appendix B: Related Aberdeen Research & Tools</i>	32



Figures

Figure 1: The top security risks that influence endpoint security solution decisions.....	iii
Figure 2: Adequacy of endpoint data protection solutions currently in place within companies.....	6
Figure 3: Top security risks influencing endpoint security decisions.....	7
Figure 4: Corporate computers containing sensitive data that have been lost, stolen, or improperly disposed of within the past year	8
Figure 5: The top business drivers influencing endpoint security decisions	8
Figure 6: The top challenges when implementing an endpoint security solution.....	10
Figure 7: Laggard frequency of measuring endpoint compliance to security policy	11
Figure 8: How companies overcame implementation challenges.....	11
Figure 9: The importance of dynamic data control based on classification	12
Figure 10: Companies that have classified and identified sensitive data.....	13
Figure 11: The adequacy at which organizations follow formal procedures to erase data when disposing of corporate computers / servers	13
Figure 12: The importance of various endpoint data risks.....	14
Figure 13: The teams involved in developing an endpoint data protection strategy	15
Figure 14: The percentage of IT staff companies would dedicate to updating endpoint security policy definitions on an ongoing basis.....	15
Figure 15: Best in Class endpoint security technologies (planned, or currently in use)	16
Figure 16: Laggard endpoint security technologies (planned, or currently in use)	17

Figures

Figure 17: Companies with a strategy in place to protect sensitive data on endpoints	18
Figure 18: Companies adopting a multi-layer approach to endpoint data protection	18
Figure 19: Data protection on specific endpoint classes	19
Figure 20: Top reasons for rejection of an endpoint data protection solution	20
Figure 21: The frequency at which endpoint compliance to data privacy and security policy measured at Best in Class and Laggard companies	20
Figure 22: How companies characterize their ability to assess the compliance of end users to endpoint and data privacy policies	21
Figure 23: Endpoint Data Protection solutions currently in use at Best in Class companies	24

Tables

Table 1: Endpoint Data Protection Challenges and Responses	9
Table 2: The endpoint data protection competitive framework	22
Table 3: Endpoint technology investments planned in the next 12 months	23
Table 4: PACE (Pressures, Actions, Capabilities, Enablers)	24
Table 5: PACE Framework	30
Table 6: Relationship between PACE and Competitive Framework	30
Table 7: Competitive Framework	30



Chapter One: Issue at Hand

Key Takeaways

- Due to the large number of endpoints that need to be protected, along with the large amounts of data at rest and in motion, organizations are finding that protecting endpoints is growing increasingly difficult.
- Key decision makers are bringing together cross-functional teams when planning endpoint data protection strategies
- A number of endpoint data protection strategies exist to mitigate the threat of loss, misuse, and abuse of data. These technologies include file or device-based encryption, information leak protection, device and application control, disk protection, and key management.
- Organizations need to take action now by implementing endpoint data protection controls, to not only gain visibility, but also to reduce the risk of a compliance failure and the loss of intellectual property.

The ever changing and evolving world of information technology, and the growing requirement on companies to protect their most valuable and sensitive information, is forcing organizations to evaluate how end-users are keeping track of, and ultimately protecting, their devices. From laptops and desktops, to the hard disks found on those machines, to removable media devices that can be easily lost or stolen; companies are finding that protection of these endpoints is growing increasingly difficult.

In response to these threats, many companies are actively looking for solutions to address security and protection of their data in motion on endpoint devices. Companies today are focused on meeting regulatory requirements, ensuring protection of personal and private data, complying with internal security policies, remediation of security issues, and are more deeply evaluating the risk around their most critical asset in the enterprise — intellectual property.

With this thought ingrained in their minds, key decision makers are taking ownership in data protection strategies by bringing together cross-functional teams with a goal of linking endpoint compliance to business compliance. Enterprises are trying to gain more visibility into their data security and to understand the potential loss vectors. The end goal is a multi-layer data protection strategy which spans all business units and involves full support from all organizational tiers, not just IT operations and security. If organizations cannot achieve this endpoint data protection goal, they are jeopardizing their security and competitive edge.

Luckily, companies in today's market have a host of cutting-edge technologies to assist in the formulation of a comprehensive endpoint data protection strategy. Everything from file or device-based encryption, to information leak protection, device and application

Competitive Framework Key

The Aberdeen Competitive Framework defines enterprises as falling into one of the three following levels of practices and performance:

Laggards (30%)—practices that are significantly behind the average of the industry

Industry norm (50%)—practices that represent the average or norm

Best in class (20%)—practices that are the best currently being employed and significantly superior to the industry norm

control, disk protection, and key management can be used to mitigate the threat of data loss, misuse, and abuse at the endpoint. Best in Class companies are in agreement that a sound data protection strategy using these technologies is now critical to the success of most businesses. In fact, only industry Laggards (see the Competitive Framework Key) have completely failed to address the issue of data protection within their enterprise.

PACE Key — For more detailed description see Appendix A

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:

Pressures — external forces that impact an organization’s market position, competitiveness, or business operations

Actions — the strategic approaches that an organization takes in response to industry pressures

Capabilities — the business process competencies required to execute corporate strategy

Enablers — the key functionality of technology solutions required to support the organization’s enabling business practices

There is significant financial risk associated with allowing critical data pass outside of the corporate network and through public networks, unapproved devices, and into the hands of customers, vendors and guests, without appropriate endpoint data protection. For example, a typical enterprise can transmit hundreds or thousands of documents containing intellectual property outside of the enterprise on an hourly basis. Any one of these documents, in the wrong hands, could harm a business, affect loss of business advantage, or expose sensitive data. When asked about the total cost of a loss event, study respondents indicated it can cost thousands in direct revenue loss, productivity loss, and fines and legal costs.

For many organizations, once the enormous cost of meeting or exceeding state and federal regulatory compliance regulations is added to the total cost of a loss event, what is left is a significant number which greatly exceeds the initial deployment and maintenance costs of a data protection solution implementation. So, although most agree that security ROI is difficult to prove, the ability to prevent a data loss event is at least compelling.

By operating in a blind mode, IT organizations continue to lack visibility and understanding of their critical data flow and they increase the risk of losing their data through unintended methods. Organizations need to take action in order to gain greater visibility into the location of their sensitive data, to understand the typical authorized use pattern of that data, and to protect it appropriately. Use of the endpoint data protection solutions can assist in this endeavor by allowing organizations to ensure that protected data at rest stays at rest, and protected data in motion stays in motion, but always through authorized channels, and always with a comprehensive level of protection. In addition, use of endpoint data protection solutions can help to guarantee a high level of security policy and regulatory compliance across a business.



Chapter Two: Key Business Value Findings

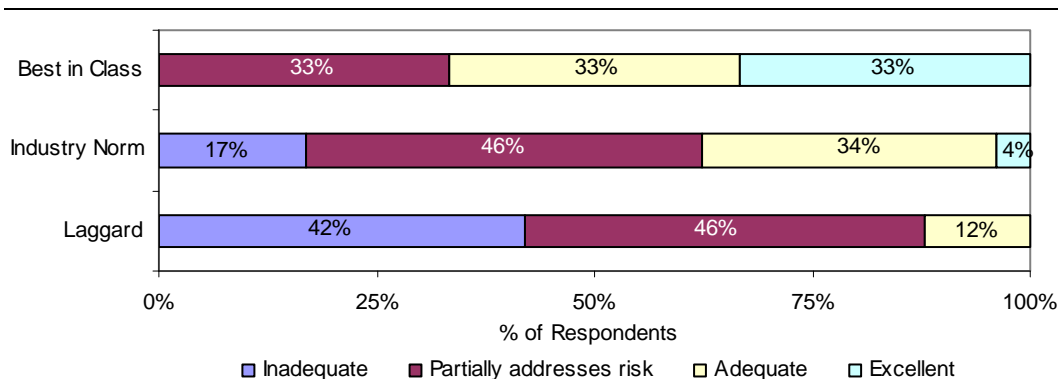
Key Takeaways

- In implementing endpoint data protection solutions, organizations are challenged by the potential impact to current systems and gaining an understanding of regulatory or security policy requirements
- Best in Class companies are successfully deploying endpoint data protection solutions, and are realizing benefits through reduced risk and enhanced compliance
- Best in Class companies are better able to assess their endpoint compliance to data privacy and security policy through the enhanced auditing and report management of endpoint data protection solutions

Recent publicity about corporate data loss has generated a lot of attention at the executive level within today's enterprises. Data no longer resides under lock and key on a single company server; only available to those internal to the organization. With the increasing use of email, instant messaging, and removable media, corporate sensitive data has more potential to be mobile, and thus is more at risk, than ever before.

Decision makers are beginning to understand the risk presented in today's work-world scenario, and are now trying to address these risks. A number of organizations have some data protection solutions in place, but, by and large, companies across the board agree that they need to improve their solutions to do a better job of addressing data and intelligence loss risks (Figure 2).

Figure 2: Adequacy of endpoint data protection solutions currently in place within companies



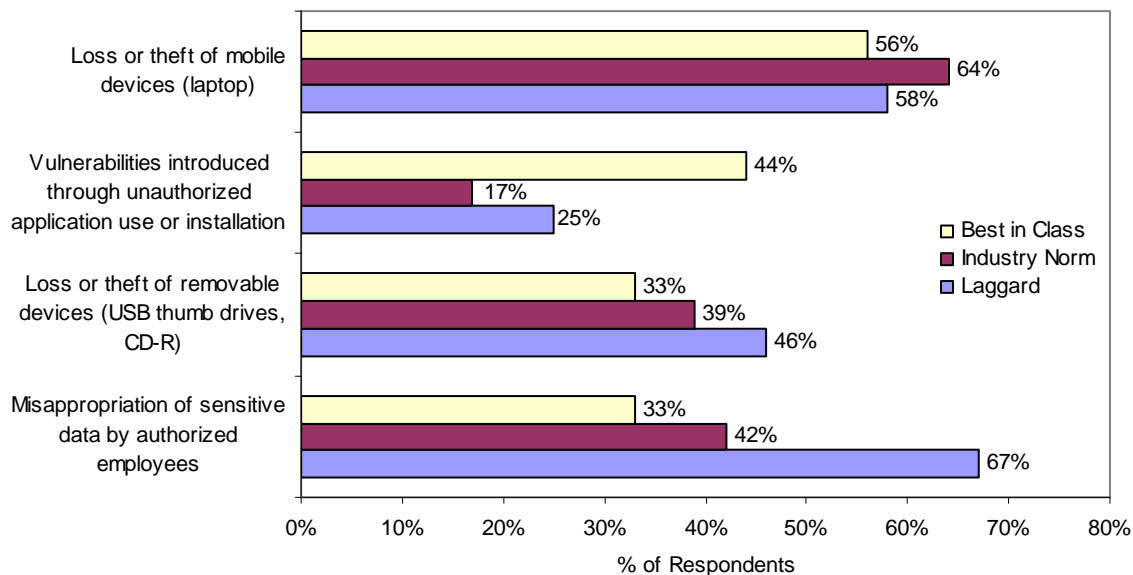
Source: Aberdeen Group, December 2006

Data protection risks areas

There are a number of problem or risk areas that decision makers have in view (Figure 3). Best in Class companies are most concerned with loss or theft of mobile devices (such

as laptops), followed by vulnerabilities introduced through unauthorized application use or installation, loss or theft of removable devices (such as USB thumb drives, CD-R), and misappropriation of sensitive data by authorized employees.

Figure 3: Top security risks influencing endpoint security decisions



Source: Aberdeen Group, December 2006

In particular, it's interesting that Laggard companies are most concerned with the risk of misappropriation of sensitive data by authorized employees. The data shows a link between this misappropriation risk, adequacy of current endpoint data protection solutions, and training. Coincidentally, 88% of Laggard companies report that their existing endpoint data protection solutions either only partially reduce the risk or are inadequate in reducing risks altogether. Only 27% of Laggard respondents indicate training staff to understand regulatory requirements, policies and best practices is a priority in overcoming endpoint data protection implementation challenges.

Theft of desktop machines or servers is getting particular media attention since the Veterans Administration had a laptop containing personal information of 26.5 million veterans stolen from an employee's home last May. The laptop did not have endpoint data protection software installed prior to the theft meaning that the personal data was open, unprotected, and at risk.

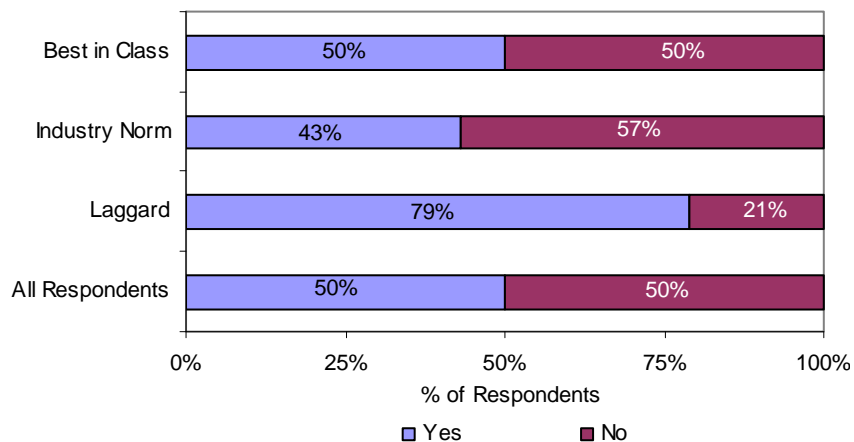
Encryption was considered a couple of years ago but it took a data loss incident to get funding for 2007.
 — IT Staff, Communications Services Industry

4).

Although the public may have had the impression that this was a one-off incident, the data from Aberdeen's study shows an entirely different picture. Surprisingly, 50% of respondents report losing — or worse, intentionally disposing of — a corporate resource containing unprotected sensitive data (Figure



Figure 4: Resource with sensitive data lost, stolen, or improperly disposed



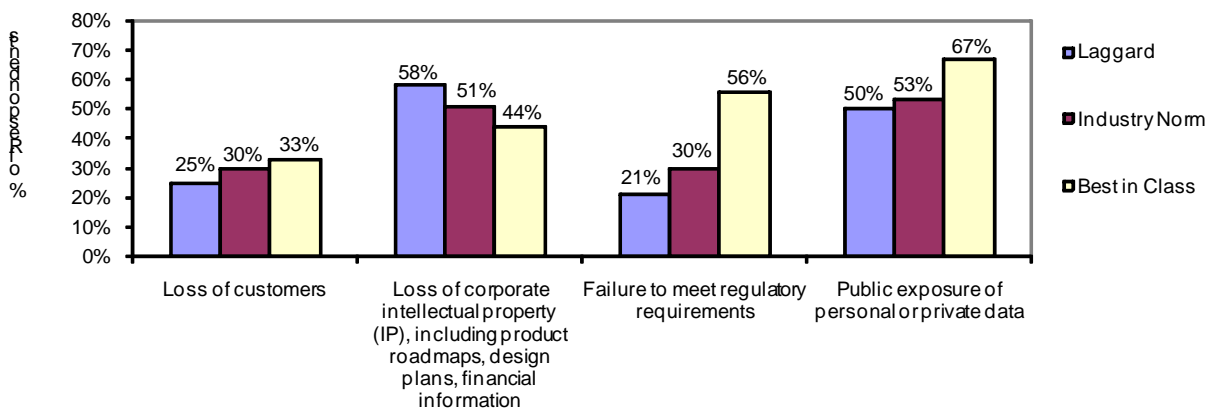
Source: Aberdeen Group, December 2006

In particular, Laggards are the worst offenders: 79% report a corporate endpoint, containing sensitive data and without appropriate data protection software, was lost, stolen, or improperly disposed.

Why is endpoint data protection so important?

Data is every organization’s lifeblood. It is the product of countless employee-hours of work and a significant monetary investment. Companies need to care for, track, and protect their data just as much as any other corporate asset. To gauge why companies are considering endpoint data protection, Aberdeen asked study respondents to rank the top business drivers for implementation of the solution (Figure 5).

Figure 5: The top business drivers influencing endpoint security decisions



Source: Aberdeen Group, December 2006

Best in Class companies are most concerned by public exposure of personal or private data (67%), followed by failure to meet regulatory requirements (56%). They are also

very concerned about loss of corporate intellectual property (IP), including product roadmaps, design plans, and financial information (44%). For Best in Class companies, the cost of remediation of a lost, stolen, or improperly disposed of endpoint containing sensitive data has no influence in the decision to implement an endpoint security solution. It's interesting to note that Laggard companies are most concerned with loss of corporate intellectual property (IP), including product roadmaps, design plans, and financial information (58%) yet they are doing the least to insulate themselves from this risk.

Security incidents seem to be occurring with greater frequency and severity.
 — Chief Information Officer,
 Manufacturing Company in the
 Metals Industry

Challenges and Responses

A number of our respondents have started down the road of advocacy for an endpoint data protection and security solution, but are encountering numerous challenges (Figure 6, Table 1).

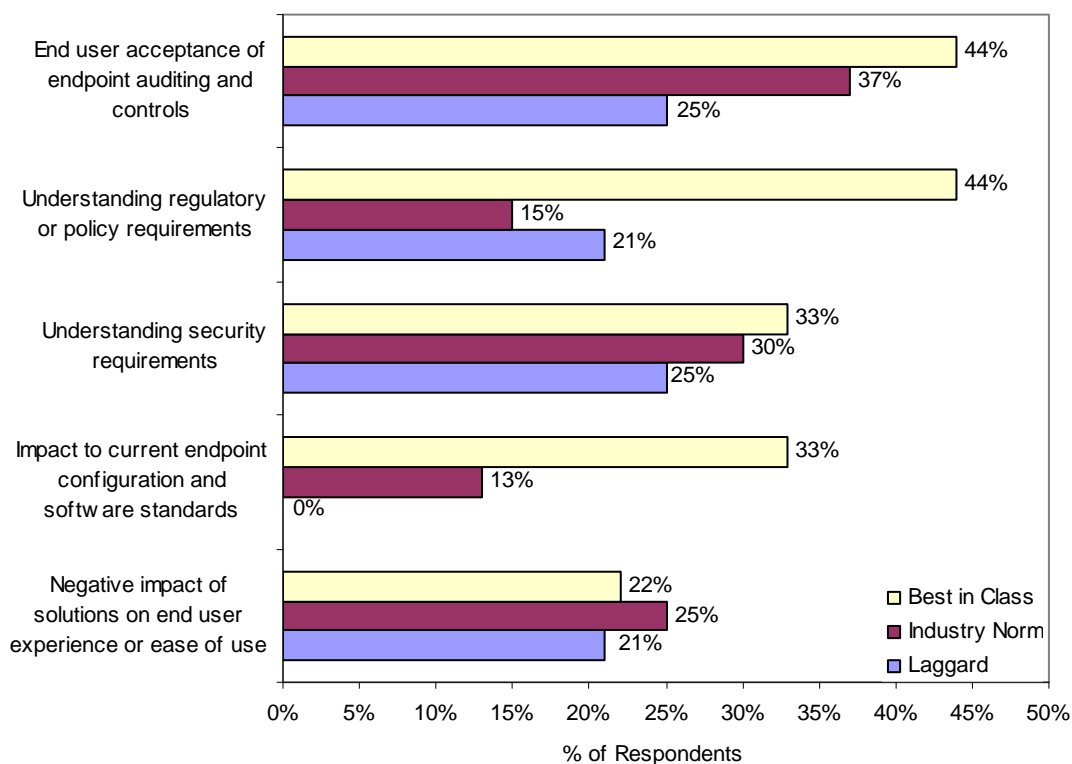
Table 1: Endpoint Data Protection Challenges and Responses

Challenges	% Selected	Responses to Challenges	% Selected
1. End user acceptance of end-point auditing and controls	44%	1. Training staff to understand regulatory requirements, polices and best practices	78%
2. Understanding regulatory or policy requirements	44%	2. Select solutions that integrate with current IT management systems (workflow, etc.)	56%
3. Understanding security requirements	33%	3. Improving / creating operational procedures and best practices	44%
4. Impact to current endpoint configuration and software standards	33%	4. Select systems that allow centralized policy definition and enforcement	33%
5. Negative impact of solution on end user experience or ease of use	22%	5. Improving integration of currently deployed endpoint security systems	33%
6. Lack of defined processes to address endpoint security	22%	Deploying automated systems to monitor and enforce endpoint security policies	22%

Source: Aberdeen Group, December 2006



Figure 6: The top challenges when implementing an endpoint security solution

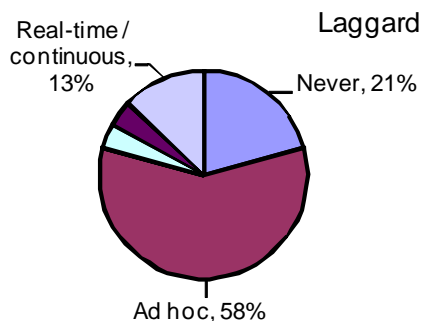


Source: Aberdeen Group, December 2006

Best in Class companies are having a particularly difficult time gaining end user acceptance of endpoint auditing and controls (44%) and understanding regulatory or policy requirements (44%). Thirty-three percent of Best in Class respondents report understanding security requirements is a challenge when implementing these solutions. Best in Class companies are also reporting challenges concerning negative impact of solutions on end user experience or ease of use (21%). Laggard companies are very concerned about understanding security requirements and end-user acceptance of endpoint auditing and control (25%). Clearly, concern does not equal action as 79% of Laggard companies are reporting they are either using Ad Hoc methods, or doing nothing at all, in measure endpoint compliance to data privacy and security policy (Figure 7).

Best in Class companies are having a particularly difficult time gaining end user acceptance of endpoint auditing and controls and understanding regulatory or policy requirements.

Figure 7: Laggard frequency of measuring endpoint compliance to security policy

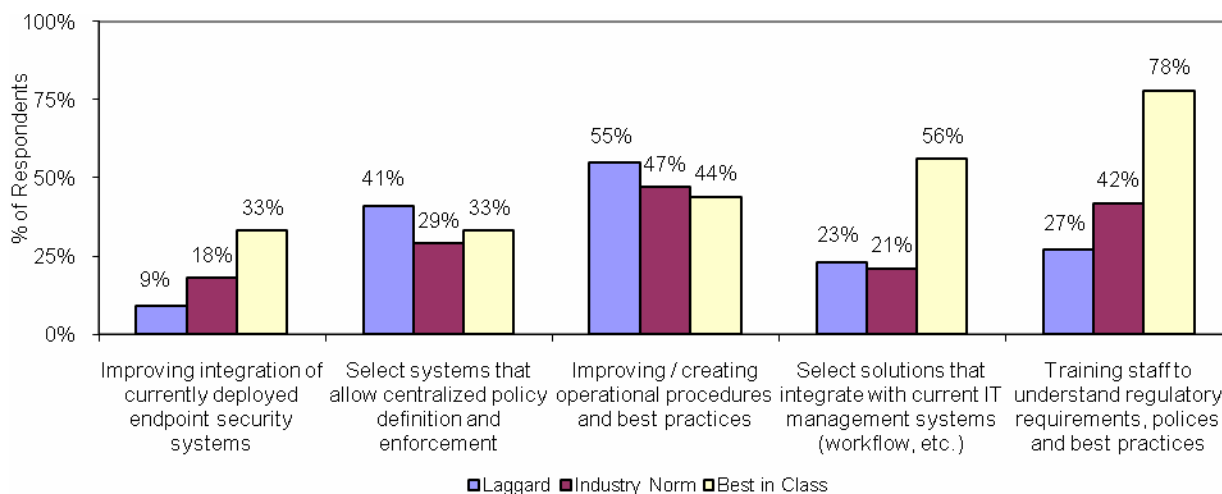


Source: Aberdeen Group, December 2006

Many respondents have been successful in overcoming the numerous challenges involved in advocating and integrating endpoint data protection solutions into their infrastructure and business processes.

Best in Class companies (Figure 8) concentrated mostly on training staff in regulatory requirements, policies, and best practices to overcome these challenges (78%). This was followed closely by selecting a solution that integrates well with current IT management systems (56%), and improving / creating operational procedures and best practices (44%). Best in Class companies also reported success in selecting systems that allow centralized policy definition and enforcement (33%) and improving integration of currently deployed endpoint security systems (33%) to improve endpoint security and drive adoption of endpoint data protection solutions. Laggards overcame their challenges by improving and/or creating operational procedures and best practices (55%), selecting systems that allow centralized policy definition and enforcement (41%), and training staff in regulatory requirements, policies, and best practices (27%) to drive adoption.

Figure 8: How companies overcame implementation challenges



Source: Aberdeen Group, December 2006



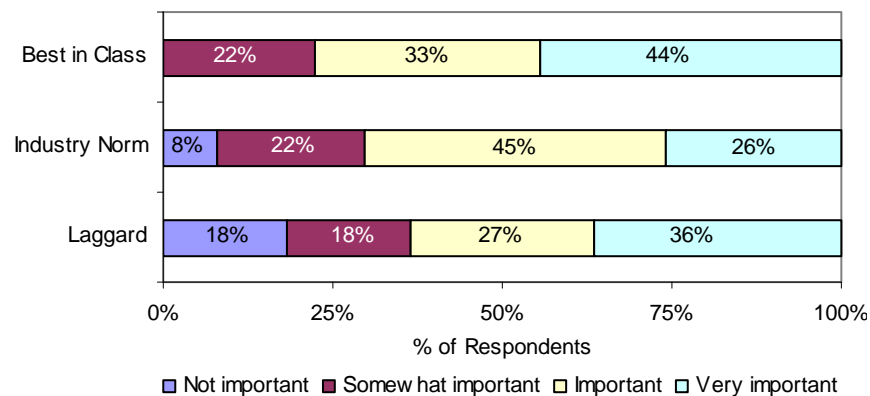
Solutions

There are a number of solutions available to step up the level of endpoint data protection. Most solutions fall into three buckets:

- 1) Data classification and inspection: useful for data on the move
- 2) Encryption: useful for stationary data, resource disposal, and data on the move
- 3) Endpoint control: policy-based control of particular sensitive data and devices

Companies are taking a new look at data classification to achieve greater accuracy in their endpoint data protection solutions (Figure 9). For example, the ability to scan the entire content and metadata of a document for a particular phrase is a key differentiator in many endpoint data protection solutions. Armed with this capability, a company can institute a more accurate security policy based on document content and context (i.e., where did the document come from, or where is it going to). These capabilities allow for easier policy deployment across the enterprise because a single policy can control flow and protect misuse of a whole set of corporate data in the same secure manner. Forty-four percent of Best in Class companies report that this capability is very important to any endpoint data protection solution. Thirty-six percent of Laggards believe that this capability is very important. Results indicate that the message is clear: dynamic data control based on classification is a key feature to endpoint data protection solutions, and it is here to stay.

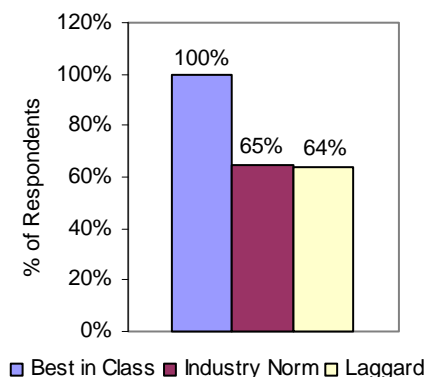
Figure 9: The importance of dynamic data control based on classification



Source: Aberdeen Group, December 2006

In Figure 10, the data shows that all Best in Class respondents report that they are successfully using data classification as part of their multi-layer approach to endpoint data protection. This further validates this capability as a key component of any multi-layer endpoint data protection strategy.

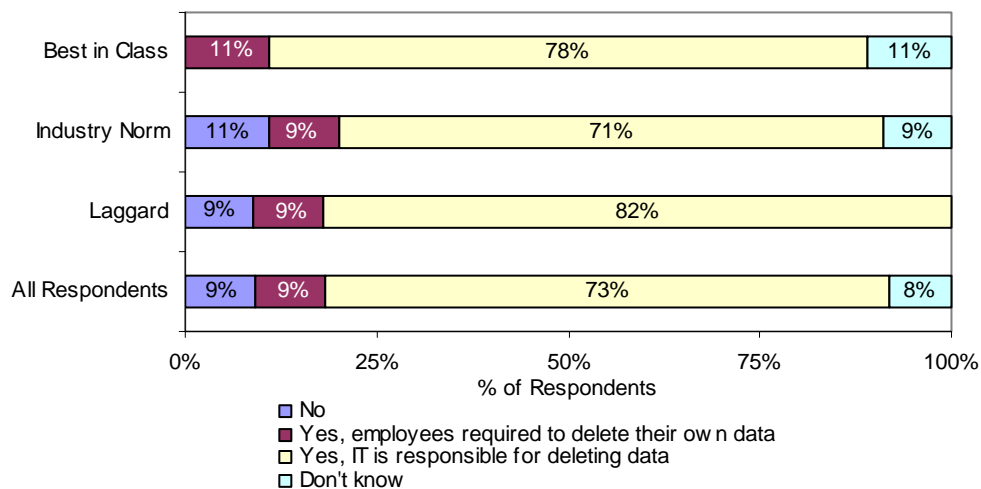
Figure 10: Companies that have classified and identified sensitive data



Source: Aberdeen Group, December 2006

Encryption solutions have a lot of flexibility when protecting enterprises from many common endpoint threats. Each year corporate America disposes of thousands of laptops, desktops, and servers. Unfortunately, as shown Figure 11, the majority of respondents are not using formal procedures to erase data when disposing of these resources. Without suitable encryption of the data on those resources, corporate sensitive data remains generally accessible to anyone who may purchase the device on the secondary market.

Figure 11: The adequacy at which organizations follow formal procedures to erase data when disposing of corporate computers / servers



Source: Aberdeen Group, December 2006

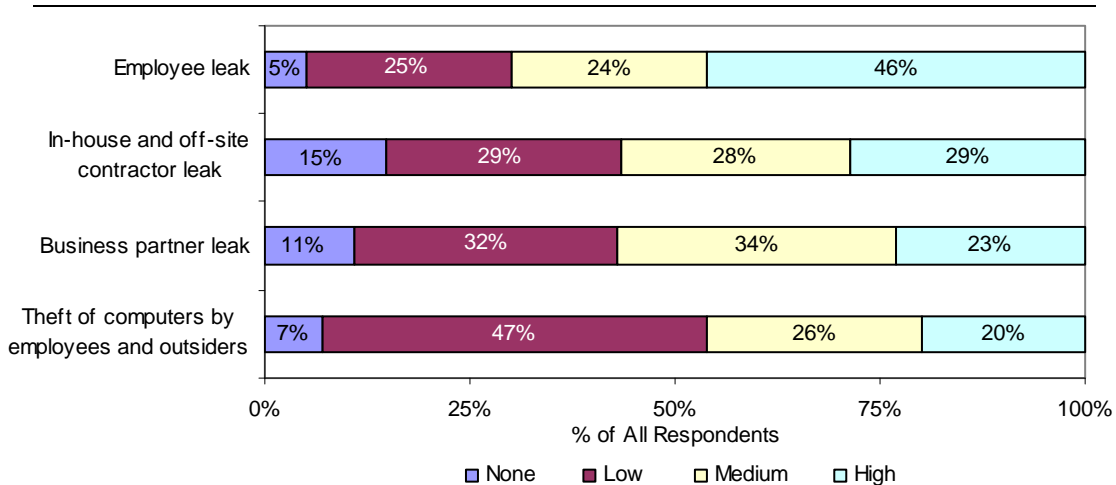
Results indicate that it isn't in the best interest of an organization to trust that all sensitive data has been erased from disposed resources. While this is a risk for all respondents, Laggards, in particular, should be concerned — 82% report IT is exclusively responsible for deleting data prior to disposal of the resource. But, without oversight, will it ever happen? Without a full disk encryption solution in place, sensitive corporate data will be



recoverable, and fully available for anyone to read. This is a competitive disadvantage for any organization. Disk encryption is the answer for this endpoint data protection threat.

Encryption is also a key solution that enables companies to protect sensitive corporate data on the move. Whether the data is emailed, copied to a removable media device, or sent through instant messenger to a colleague, friend, or worse, competition, data in motion represents a significant problem for most of the companies studied. Figure 12 shows how respondents evaluated the importance of various data-in-motion risks.

Figure 12: The importance of various endpoint data risks



Source: Aberdeen Group, December 2006

It's interesting to note that across all respondents surveyed, 46% indicate that an employee leak is the highest risk for endpoint data. This is followed by contractor leaks (29%), business partner leaks (23%), and theft of computers by employees and outsiders (20%). These numbers back up the need for an endpoint data protection solution which can enact specific encryption policies on a per-user or per-machine basis.

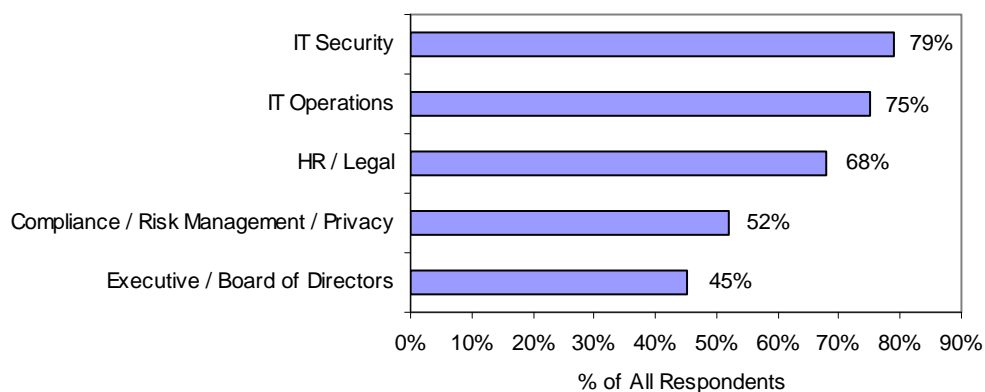
Since our outside sales force has a database that is synchronized with our servers, containing customer information like product sales, pricing, and call reports, it would be imperative that we be able to secure this information.

— Chief Information Officer, Manufacturing Company in the Metals Industry

How to get started

When effectively planning an endpoint data protection strategy, our respondents were successful in involving cross-functional teams within the enterprise to better understand the problem. Figure 13 shows the top five functional areas involved in planning endpoint and data privacy security requirements.

Figure 13: The teams involved in developing an endpoint data protection strategy

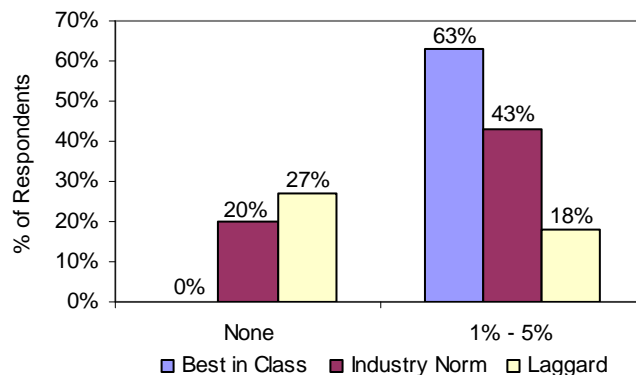


Source: Aberdeen Group, December 2006

Unsurprisingly, IT security (79%) and IT operations (75%) top the list, followed by human resources / legal (68%), compliance / risk management / privacy (52%), and executive / board of directors (45%) rounding out the top five.

Data is constantly changing, and in order to keep up, any endpoint data protection solution will require some level of policy adjustment or update to work in an efficient manner. As a result, when planning an endpoint data protection solution, consider the staffing level (and hours of work) required to maintain the security policy definitions on an ongoing basis. Consider Figure 14, which shows that organizations are resource-strapped and dedicated resources to maintain endpoint security policy definitions often do not exist.

Figure 14: The percentage of IT staff companies would dedicate to updating endpoint security policy definitions on an ongoing basis



Source: Aberdeen Group, December 2006

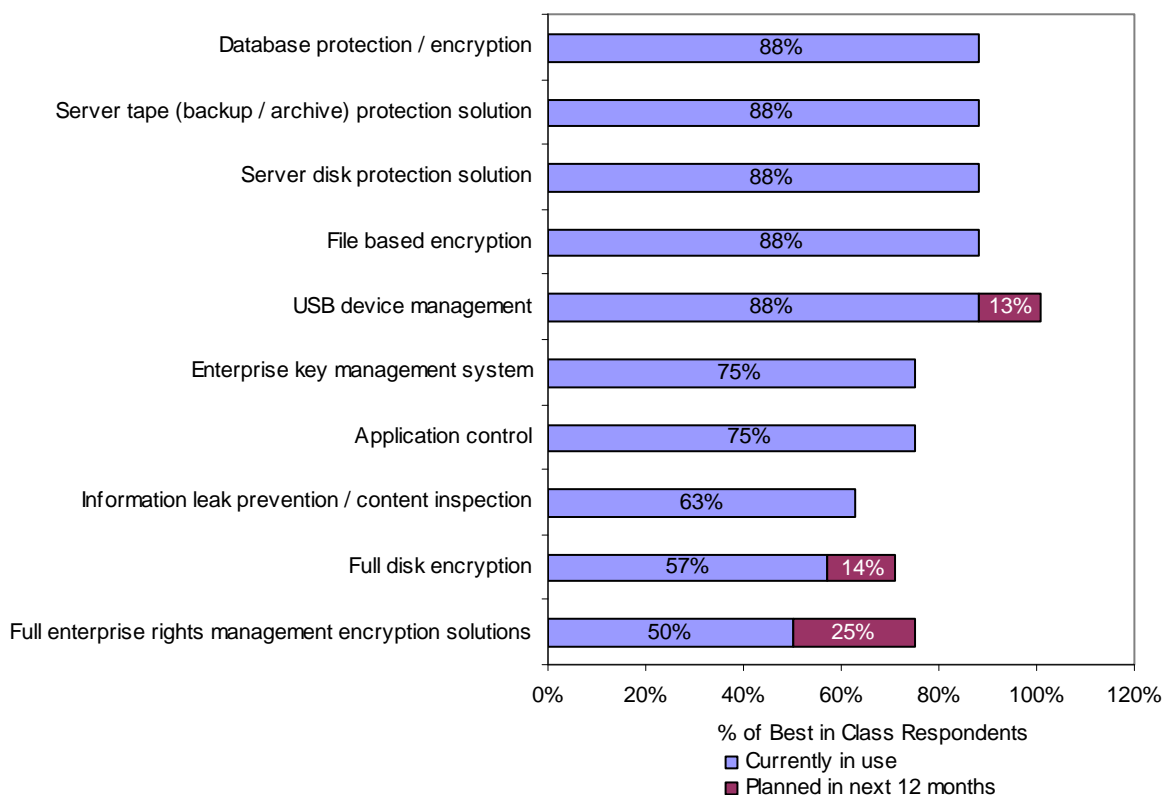
In fact, the most common response was that companies could only dedicate 1% to 5% of their staff to updating endpoint security policy definitions on an ongoing basis. This proves that any workable endpoint data security solution will have to incorporate a large degree of automation, a clear reporting engine, and a concise policy engine which can



make policy change suggestions based on constantly changing risk profiles within the enterprise.

Aberdeen recommends speaking with the members of cross-functional business teams about their needs for the system, and after gaining an understanding of who will own the maintenance and upkeep of the solution, determine which solution will be most appropriate for the organization's particular needs. Study respondents indicated that there are many solution categories which have some overlap. The following figures show some of the most popular solutions categories, and are broken up by "solutions currently in use" and "solutions planned for use in the next 12 months." The Best in Class respondents are represented in Figure 15.

Figure 15: Best in Class endpoint security technologies (planned, or currently in use)

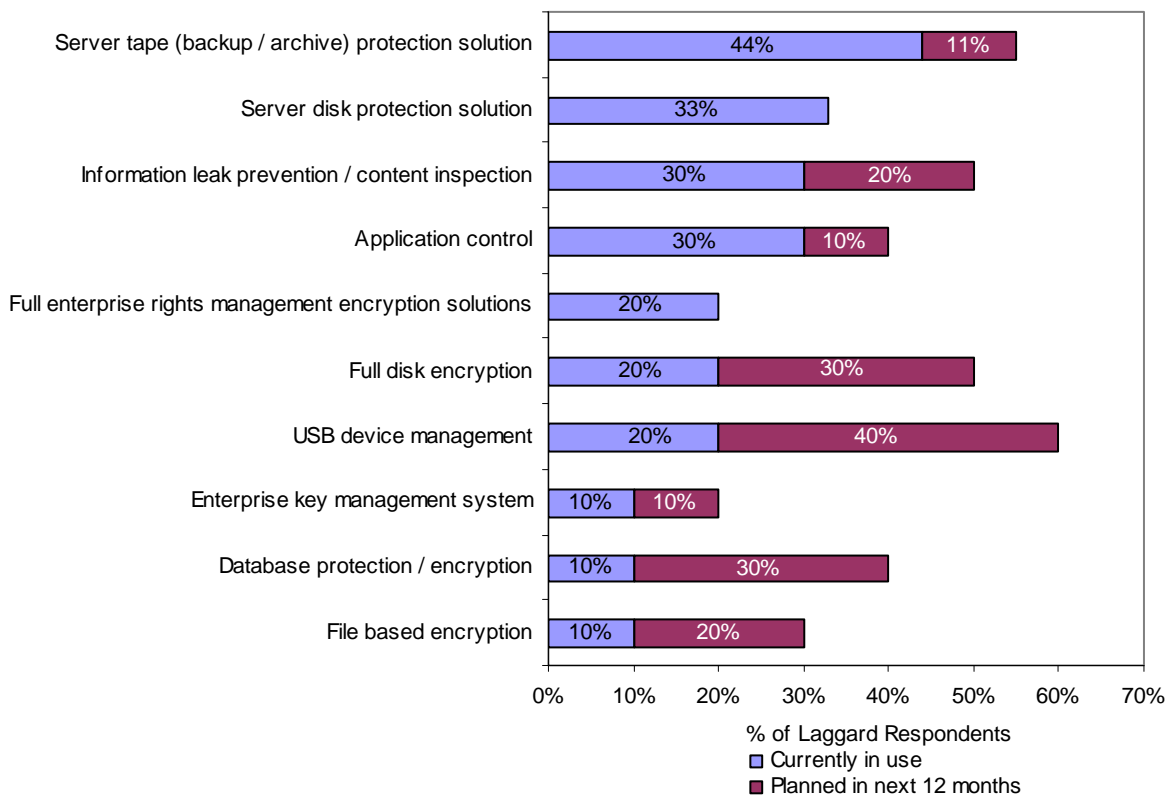


Source: Aberdeen Group, December 2006

The data shows that Best in Class respondents are generally using database protection/encryption (88%), server tape (backup/archive) protection (88%), server disk protection (88%), file-based encryption (88%) and USB device management (88%). Over the next 12 months, 25% of Best in Class respondents are planning to implement full enterprise rights management encryption solutions, while 14% are planning to implement full disk encryption, and 13% are planning on implementing USB device management solutions.

Laggard respondents (Figure 16), in comparison to Best in Class respondents, currently use less technology but have aggressive plans for implementation in the next 12 months. For Laggard respondents, USB device management (40%) leads the solutions that are planned for implementation, followed by full disk encryption (30%) and database protection / encryption (30%). ILP (20%), file based encryption (20%), server tape protection (11%), enterprise key management system (10%), and application control (10%) conclude the list.

Figure 16: Laggard endpoint security technologies (planned, or currently in use)



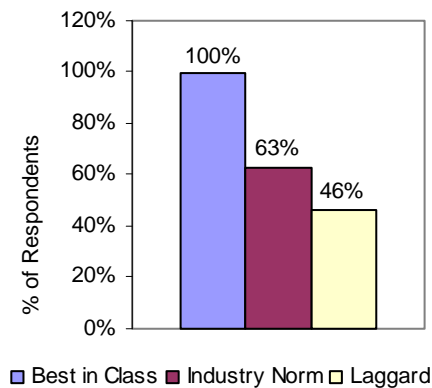
Source: Aberdeen Group, December 2006

Strategies for those already using endpoint data protection solutions

Unsurprisingly, Best in Class companies (Figure 17) report the highest current usage of endpoint data protection solutions.



Figure 17: Companies with a strategy in place to protect sensitive data on endpoints

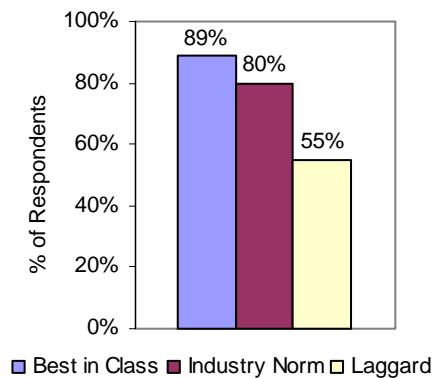


Source: Aberdeen Group, December 2006

In turn, Best in Class companies are best prepared to protect their sensitive data from all risks, including theft, misuse, or loss.

Most respondents generally agree that a multi-layer strategy is the best approach to endpoint data security protection (Figure 18).

Figure 18: Companies adopting a multi-layer approach to endpoint data protection

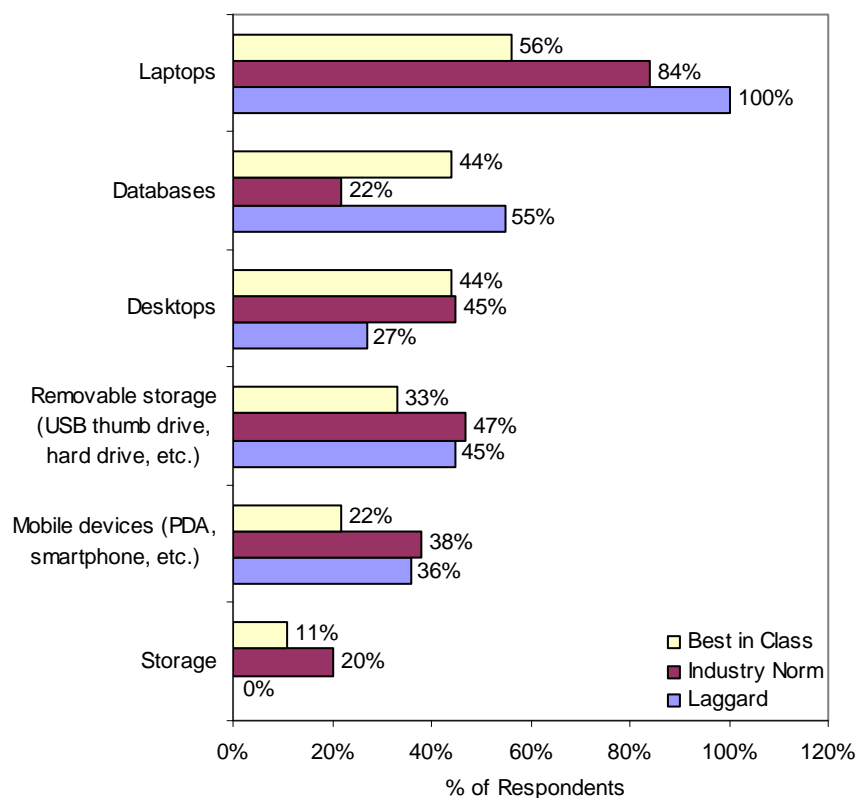


Source: Aberdeen Group, December 2006

Best in Class respondents (89%) are the staunchest advocates of this approach, followed logically by Industry Norm (80%), and Laggard (55%).

To determine which industry segments were routinely protecting all endpoint resources within their enterprises, data results from the Best in Class were examined. The results are shown in Figure 19.

Figure 19: Data protection on specific endpoint classes



Source: Aberdeen Group, December 2006

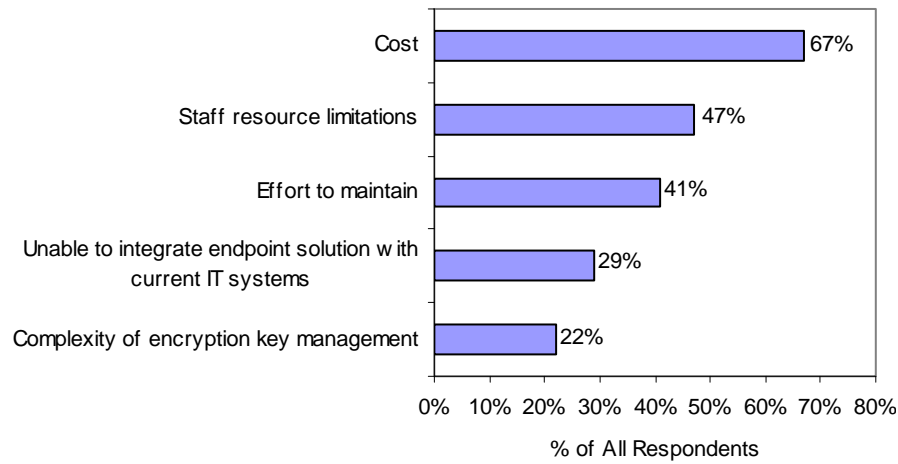
The results show that Best in Class respondents are most likely to be using endpoint data protection solutions on their laptops, databases, desktops, and removable storage. But, for future protection, they need to consider deploying endpoint data protection to both mobile devices and storage. Laggards, on the other hand, are 100% focused on endpoint protection of laptops, followed by databases, removable storage, mobile devices, and desktops.

Solution Satisfaction

To better understand what is needed to improve vendors’ endpoint data protection solutions, respondents were asked about the reasons why they considered, but rejected, an endpoint data protection solution. Figure 20 shows the top responses.



Figure 20: Top reasons for rejection of an endpoint data protection solution

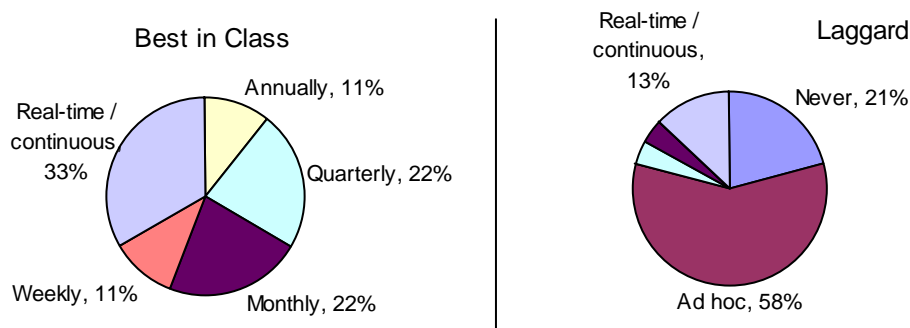


Source: Aberdeen Group, December 2006

Cost came in as a leading factor (67%), followed by staff resource limitations (47%), effort to maintain (41%), inability to integrate endpoint solution with current IT systems (29%), and complexity of encryption key management (22%).

The majority of those respondents currently using an endpoint data protection solution are happy with the results. The data represented in Figure 21 shows that 66% of Best in Class companies are measuring endpoint compliance to data privacy and security policy at least monthly. What is even more impressive is that 33% of Best in Class respondents are monitoring compliance in real-time.

Figure 21: The frequency at which endpoint compliance to data privacy and security policy measured at Best in Class and Laggard companies

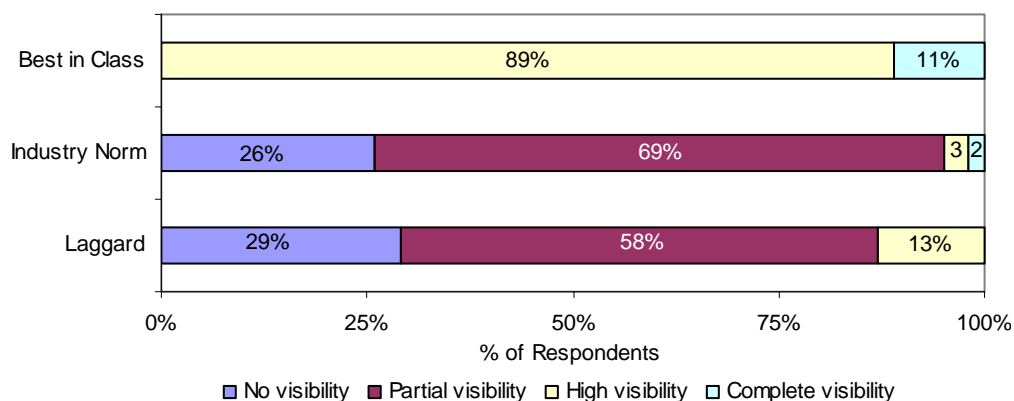


Source: Aberdeen Group, December 2006

Laggards, for the most part, are not using endpoint data protection solutions, and are mostly using ad hoc methods of monitoring endpoint compliance to data privacy and security policy.

A real measure of satisfaction of endpoint data protection solutions is how well it has allowed companies to gain visibility into the security risks in their environment. Figure 22 highlights that Best in Class companies are showing impressive results.

Figure 22: How companies characterize their ability to assess the compliance of end users to endpoint and data privacy policies



Source: Aberdeen Group, December 2006

Best in Class companies are reporting either high or complete visibility into the compliance of end users to endpoint and data privacy policies. This is an excellent result and speaks volumes for the successful multi-layer endpoint data protection and security strategy in use at most Best in Class organizations.



Chapter Three: Implications & Analysis

Key Takeaways

- Best in Class organizations proactively involve cross-functional teams in planning their endpoint data protection solutions.
- Best in Class organizations view loss or theft of mobile devices as a major risk.
- In making decisions about endpoint security solutions, Best in Class organizations are most influenced by loss or theft of mobile devices (such as Laptops).
- Best in Class companies were most able to overcome endpoint data protection challenges through training staff to understand regulatory requirements, policies, and best practices.

As shown in Table 2, survey respondents fell into one of three categories — Laggard, Industry Average, or Best in Class — based on their characteristics in four key categories: (1) process (of planning endpoint data protection); (2) organization (current organizational endpoint protection capabilities); (3) knowledge (visibility into data loss, misuse, and abuse); and (4) technology (scope of endpoint data protection tools).

In each of these categories, survey results show that the firms exhibiting Best in Class endpoint data protection characteristics also enjoy Best in Class security, control, and visibility.

Table 2: The endpoint data protection competitive framework

	Laggards	Industry Average	Best in Class
Process	Endpoint data protection strategy is not in place	Endpoint data protection strategy is being planned	Endpoint data protection solutions are being proactively implemented
Organization	There is little control over sensitive data flow out of the organization	There is some security and control over sensitive data flow out of the organization	There is complete, real-time security and control over sensitive data flow out of the organization
Knowledge	There is limited visibility into endpoint sensitive data loss, misuse, or abuse	There is some visibility into endpoint sensitive data loss, misuse, or abuse	There is real-time visibility into endpoint sensitive data loss, misuse, or abuse
Technology	Manual processes are being used, and an ad-hoc methodology is being used to assess compliance	There are some automated processes, but the sophistication required to effectively report status for regulatory reasons is lacking	There is full automation of the endpoint data protection solution, and easy-to-use integrated auditing and report management capabilities

Source: Aberdeen Group, December 2006

Process and Organization

- In the process category, firms that proactively involved cross-functional business units in endpoint data protection policy development consistently had less data loss events than firms that have no visibility or teamwork on policy development.
- All Best in Class firms have a strategy to protect data stored and used on endpoints, and 89% of those firms are adopting a multi-layer strategy to address endpoint data protection; versus Laggard firms with an endpoint data protection strategy (only 46% report having a strategy and 45% report it is not multi-layered). As a result, all Laggard firms are reporting an increase in data loss incidents over the past two years. Unsurprisingly, firms reporting an increase in data loss events are also reporting that their endpoint data protection solutions are inadequate or only partially adequate.

Firms that involve cross-functional teams in early policy development consistently had less data loss events.

Technology Use

Across all studied industry categories, USB Device Management (21%) is the leading technology solution investment category (Table 3), with Full Disk Encryption (16%), Server Tape Backup/Archive Protection (13%), Information Leak Protection/Content Inspection (12%), and file based encryption (12%) rounding out the top five planned investments.

Table 3: Endpoint technology investments planned in the next 12 months

Technology Solution Area	% Selected
USB Device Management	21%
Full Disk Encryption	16%
Server tape backup/archive protection solution	13%
Information Leak Prevention / Content Inspection	12%
File based encryption	12%

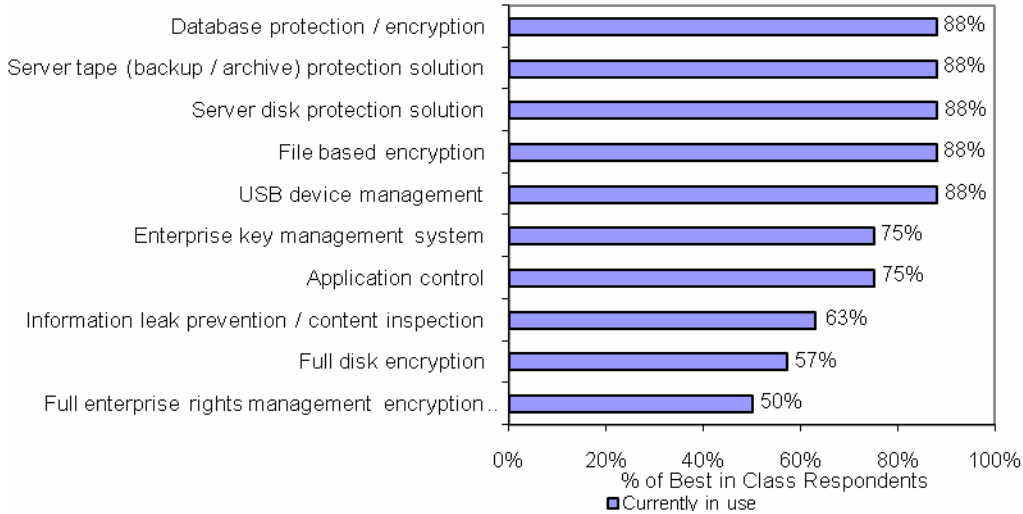
Source: Aberdeen Group, December 2006

Security Solutions Currently In Use

A number of the Best in Class companies studied are currently using endpoint data protection technologies, in addition to a number of other products, to address their needs (Figure 23).



Figure 23: Endpoint Data Protection solutions currently in use at Best in Class companies



Source: Aberdeen Group, December 2006

Pressures, Actions, Capabilities, Enablers (PACE)

Data results show that there is a clear relationship between the pressures companies identify, the actions they take in response to those pressures, and their subsequent competitive performance. Companies should all examine the prioritized PACE selections and determine whether there are valuable perspectives to be gleaned by comparison with the PACE priorities of Best in Class companies.

Table 4: PACE (Pressures, Actions, Capabilities, Enablers)

Priorities	Prioritized Pressures	Prioritized Actions	Prioritized Capabilities	Prioritized Enablers
1	Achieve endpoint compliance with policy enforcement	Create and distribute endpoint policies that analyze the security state and assist in threat remediation	Leverage existing technologies to gain a better understanding of highest risk endpoints	Implement endpoint data protection solutions that allow for a high degree of automation, particularly for remediation
2	Adapt solutions to changing threats	Create a plan to regularly review security requirements and update endpoint data protection policies and definitions to reflect new changes	Involve business units outside of IT security and operations to get a better sense of the risks across the enterprise	Select an endpoint data protection solution which allows for enhanced risk and threat reporting to further enhance visibility

Priorities	Prioritized Pressures	Prioritized Actions	Prioritized Capabilities	Prioritized Enablers
3	Getting end users to accept endpoint data protection solutions	Involve business units outside of IT security and operations to select a solution which best needs the needs of the entire enterprise	Utilize cross functional teams, including end-users, who will be most affected by the endpoint data protection policies, and add material to training programs to underscore the importance of enforcing endpoint security	Implement security solutions that are automated and provide as little impact as possible to current business processes. Automated remediation of security threats should include feedback (for end users of the security policy) about violation details, and who to contact with questions

Source: Aberdeen Group, December 2006

Business Impact of Endpoint Data Protection Solutions

Endpoint data protection solutions are particularly rich candidates for leveraging the impact beyond the traditional areas of IT security and information loss. Utilizing effective endpoint data classification, encryption, and control solutions that prevent the loss of sensitive corporate data via misuse or abuse translates to significant savings in business costs by reducing risk and improving compliance. Adoption of endpoint data protection solutions that are easily integrated into the existing infrastructure, and allow for some automation of resolution remediation, yields real reductions in operational and training costs. Technology managers can offset any potential costs of acquiring new products by realizing these savings.



Chapter Four: Recommendations for Action

Key Takeaways

- Organizations should work toward establishing an endpoint data protection strategy which protects their intellectual property yet does not disrupt normal flow of business
- Involve additional teams in the consideration of an endpoint data protection solution. This will help you to avoid potential issues of end-user acceptance later on in the testing and deployment phases.
- Consider solutions which will integrate well with you existing infrastructure, incorporate centralized policy management and provide automatic remediation and training capabilities.

Improved security and regulatory compliance, enhanced data protection, data loss incident reduction, and increased operational efficiency benefits await all firms that are committed to implementing endpoint data protection solutions. The aggressiveness of recommended improvement activities, though, depends in large part on the organizations visibility into the end-user endpoint security policy compliance and an understanding of the security risks of data that passes through unprotected endpoints without scrutiny or security.

Whether a company is trying to gradually improve its security readiness 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

1. *Try to understand where sensitive data lives, who is authorized to use it, and where it travels. Then, create operational procedures and best practices for the protection of this sensitive data.*

It’s clear that without a basic understanding of the lifecycle of sensitive data, it will be difficult to form the framework for the procedures and policies that are critical to a successful endpoint data protection strategy.

2. *Generate management statistics and reports to support implementation of an endpoint data protection solution.*

This can be accomplished by putting together an analysis from existing infrastructure. For example, a list of all email attachments leaving the organization, and how many of those attachments were business-sensitive data.

3. *Evaluate endpoint data protection systems that prioritize centralized policy definition and automated enforcement.*

The endpoint data protection solution must incorporate the ability to have multiple policy sets applied to users, groups, and machines, and all of those policy sets must be managed from a central console employing a database and a central management and administration.

Having been involved with this sector for some years, I know that the end-users want multiple security services under one console. Managing a database and a central management and administration.

4. *Advocate chosen endpoint data protection solutions across multiple teams and management and move toward a production pilot.*

Involve cross-functional teams consisting of both management and employees in the planning of the endpoint data protection solution. The feedback they can give about their individual concerns and pain points will be invaluable to understanding where the business problems exist.

Push the vendor for a production pilot. It is critical to see this solution working in the company's unique production environment in diverse groups prior to deploying across the enterprise.

Industry Norm Steps to Success

1. *Use multiple risk data points to advocate endpoint data protection solutions.*

Consider that a loss of intellectual property can mean more than loss of competitive advantage. Help key decision makers understand that a loss event can be very visible, and can cause negative perception of the company or product in the marketplace. Also consider the potential of regulatory non-compliance incident and the potential fines and customer loss that go along with it.

The large volume of client's sensitive data that we process, including contractual requirements from clients, drove us to address the problem of endpoint data protection in our organization.
—Director of Risk Management for a business process outsourcing organization

2. *Conclude your planning and production pilot phases of the endpoint data protection solution rollout, and provide findings to key decision makers.*

The findings should include the number of sensitive documents accessed, how many of those documents left the organization, and how the endpoint data protection solution could have help reduce or eliminate this risk.

3. *Begin planning your endpoint data protection policy set, and ensure that it will address the entire scope of risk across your enterprise, while also minimizing business disruption.*

Make sure the endpoint data protection vendor provides a basic policy set out-of-the-box. Inspect this policy set, and modify it as appropriate. Policy planning needs to begin early to be better prepared for production implementation.

Best in Class Next Steps

1. *Continue to enhance endpoint data protection solutions to provide real-time reporting and risk analysis.*

Ensure that a loss event can be prevented, or immediately addressed when it happens. Knowing about a loss event later when it is too late to protect yourself or your good reputation is not acceptable.

2. *Use the analysis of end user behavior to consider new risks on the horizon and how an endpoint data protection solution can assist with these problems.*



Be proactive. Establish and/or participate in user groups to share best practices for endpoint data protection. Sharing the problems or risks companies, or business units, are seeing in their environments will help everyone involved better protect themselves from data loss or misuse.

3. *Incorporate methods of training employees on security and regulatory policy compliance into the endpoint data protection solution.*

If employees better understand security and regulatory policies, and the importance of protecting corporate sensitive data, overall organization and departmental protection will be more successful.

[Send to a Friend](#) 

Appendix A: Research Methodology

In December 2006, Aberdeen Group examined the endpoint data protection procedures, experiences, and intentions of more than 135 enterprises in high technology/software, finance/banking/accounting, computer equipment and peripherals, telecommunication services, and other industries.

Responding technology, security, and consulting executives completed an online survey that included questions designed to determine the following:

- The visibility into end user to endpoint security policy compliance
- The structure and effectiveness of existing endpoint data protection methods
- The challenges and responses to implementing an endpoint data protection solution
- The benefits, if any, that have been derived from endpoint data protection initiatives

Aberdeen supplemented this online survey effort with telephone interviews with select survey respondents, gathering additional information on endpoint data protection strategies, experiences, and results.

The study aimed to identify emerging best practices for endpoint data protection, and to provide a framework by which readers could assess their own endpoint data protection capabilities.

Responding enterprises included the following:

- **Job title/function:** The research sample included respondents with the following job titles: CEO, COO, or president (22%); manager (22%); staff (11%); director (10%); vice-president (9%); CIO (8%); consultant (6%), and other (12%).
- **Industry:** The research sample included respondents predominantly from high-technology industries. High technology/software companies represented 28% of the sample, followed by finance/banking/accounting, which accounted for 21% of respondents. Manufacturers of computer equipment and peripherals totaled 15% of respondents. Telecommunications services accounted for 11% of the sample. Other sectors responding included public sector, aerospace and defense, and transportation and logistics.
- **Geography:** North America represented 65% of respondents. Remaining respondents were from Europe (17%), the Asia/Pacific region (12%) and the Middle East region (5%).
- **Company size:** About 32% of respondents were from large enterprises (annual revenues above US\$1 billion); 24% were from midsize enterprises (annual revenues between \$50 million and \$1 billion); and 44% of respondents were from small businesses (annual revenues of \$50 million or less).



Table 5: PACE Framework

PACE Key
<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><i>Pressures</i> — 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><i>Actions</i> — 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><i>Capabilities</i> — the business process competencies required to execute corporate strategy (e.g., skilled people, brand, market positioning, viable products/services, ecosystem partners, financing)</p> <p><i>Enablers</i> — 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, December 2006

Table 6: Relationship between PACE and Competitive Framework

PACE and Competitive Framework How They Interact
<p>Aberdeen research indicates that companies that identify the most impactful 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.</p>

Source: Aberdeen Group, December 2006

Table 7: Competitive Framework

Competitive Framework Key
<p>The Aberdeen Competitive Framework defines enterprises as falling into one of the three following levels of ENDPOINT DATA PROTECTION practices and performance:</p> <p><i>Laggards (30%)</i> — ENDPOINT DATA PROTECTION practices that are significantly behind the average of the industry, and result in below average performance</p> <p><i>Industry norm (50%)</i> — ENDPOINT DATA PROTECTION practices that represent the average or norm, and result in average industry performance.</p> <p><i>Best in class (20%)</i> — ENDPOINT DATA PROTECTION practices that are the best currently being employed and significantly superior to the industry norm, and result in the top industry performance.</p>

Source: Aberdeen Group, December 2006



Appendix B: Related Aberdeen Research & Tools

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

- [Endpoint Security Strategies Part I: The Network Access Control Benchmark Report](#) (December 2006)
- [Large Companies are Taking Advantage of NAC Automation to Lessen Burdens on Existing Staff](#) (December 2006)
- [Large Companies are Most Aware of the Need to Wrap Regulatory Requirements into Security Strategies](#) (December 2006)
- [Encryption Options for Endpoint Data Protection: The File, Disk, and Device Encryption Vendor Landscape](#) (December 2006)
- [The 2006 Messaging Security Benchmark Report](#) (August 2006)
- [Messaging Security: Information Leak Prevention Vendor Landscape](#) (September 2006)

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

*Aberdeen Group, Inc.
260 Franklin Street
Boston, Massachusetts
02110-3112
USA*

*Telephone: 617 723 7890
Fax: 617 723 7897
www.aberdeen.com*

*© 2006 Aberdeen Group, Inc.
All rights reserved
December 2006*

Founded in 1988, Aberdeen Group is the technology-driven research destination of choice for the global business executive. Aberdeen Group has over 100,000 research members in over 36 countries around the world that both participate in and direct the most comprehensive technology-driven value chain research in the market. Through its continued fact-based research, benchmarking, and actionable analysis, Aberdeen Group offers global business and technology executives a unique mix of actionable research, KPIs, tools, and services.

The information contained in this publication has been obtained from sources Aberdeen believes to be reliable, but is not guaranteed by Aberdeen. Aberdeen publications reflect the analyst's judgment at the time and are subject to change without notice.

The trademarks and registered trademarks of the corporations mentioned in this publication are the property of their respective holders.