Aberdeen Group
A Harte-Hanks Company

Laptop Lost or Stolen?

Five Questions to Ask and Answer

February 2010

Derek Brink

~ Underwritten, in Part, by ~

Absolute Software

intel

WINMAGIC
DATA SECURITY
Knowing You're Protected

Executive Summary

In Aberdeen's study of over 150 organizations, for every 100 enterprise endpoints that went out only 85 came back – 5 were lost or stolen, 1 of these was successfully recovered, and 11 are missing and unaccounted for. This report highlights five key questions to help companies manage their risk and minimize their cost related to protecting and managing their endpoints.

Research Benchmark

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

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 as they relate to protecting and managing endpoint systems:

- Number of actual security-related incidents (e.g., data loss or exposure, endpoint loss or theft)
- Number of non-compliance incidents (e.g., audit deficiencies)
- Number of help desk calls

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:

- Consistent policies for protecting sensitive data in use at the endpoints (74%); systematic implementation and rollout processes for endpoint software, updates and configurations (74%)
- Responsible executive or team with primary ownership for security, compliance and management of endpoint systems (70%); formal documentation, awareness and end-user training programs (61%)
- Discovery, classification, tracking and reporting of information assets (61%); inventory, tracking and reporting of endpoints (57%)
- Standardized endpoint devices / platforms (86%); standardized configurations (82%); technical controls to lock down standard configurations (64%)
- Regular review and analysis of data from endpoint security and endpoint management systems (57%)

"Our project has been based on a three-pronged approach. First, the education of our employees about personal health information and other sensitive data, and about our policies for protecting that information on their laptops. Second, an efficient method for discovering if such information exists on their laptops. And third, providing a standard encryption solution for those cases where it does."

~ Rick Riordan, Executive Vice President of Shared Services, CedarCrestone Inc.

Recommended Actions

In addition to the specific recommendations in Chapter Three, to achieve Best-in-Class results companies should also look closely at the significant opportunities to reduce risk and save cost by reducing the net number of their endpoint systems that routinely go lost, stolen or missing.

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: Playing Chicken with Your Endpoints....5
Market Drivers and Inhibitors....7
Maturity Class Framework: Defining the Best-in-Class....8
The Best-in-Class PACE Model....9
Best-in-Class Strategies and Results....10
Chapter Two: Benchmarking Requirements for Success....14
Competitive Assessment....14
Capabilities and Enablers....16
Chapter Three: Recommended Actions....22
Define and Manage What's Supposed to Happen....22
Understand What Assets are at Risk....22
Put Appropriate Protections in Place....23
Track and Recover Endpoint Assets....23
Prevent Future Occurrences....24
Appendix A: Research Methodology....25
Appendix B: Related Aberdeen Research....27
Featured Underwriters....29

Figures

Figure 1: Where Have All the Enterprise Endpoints Gone?....5
Figure 2: Top Drivers of Current Endpoint Investments....8
Figure 3: Leading Inhibitors to Current Endpoint Investments....8
Figure 4: Top Strategies Driving Current Endpoint Investments....11
Figure 5: Consistent Policies, Standardized Processes Drive Top Results....16
Figure 6: Accountability and Planning....17
Figure 7: Identification, Tracking and Reporting on Assets....18
Figure 8: Standardization of Platforms and Configurations; Backup and Migration of Data....18
Figure 9: Making Use of Available Information....20
Figure 10: Current Use of Enabling Technologies by the Best-in-Class....21

Tables

Table 1: Importance Placed on Selected Aspects of Protecting and Managing Endpoints....7
Table 2: Top Performers Earn Best-in-Class Status....9

Table 3: Best-in-Class PACE Framework for Protecting and Managing Endpoints....10
Table 4: Benefits of Endpoint Tracking, Recovery and Deterrence....12
Table 5: Benefits of Implementing Endpoint Protections 13
Table 6: Competitive Framework for Endpoints....15
Table 7: Enabling Technologies Commonly Used in Protecting and Managing Endpoint Systems 19
Table 8: PACE Framework Key....26
Table 9: Competitive Framework Key....26
Table 10: Relationship Between PACE and the Competitive Framework....26

Chapter One:
Benchmarking the Best-in-Class

Business Context: Playing Chicken with Your Endpoints

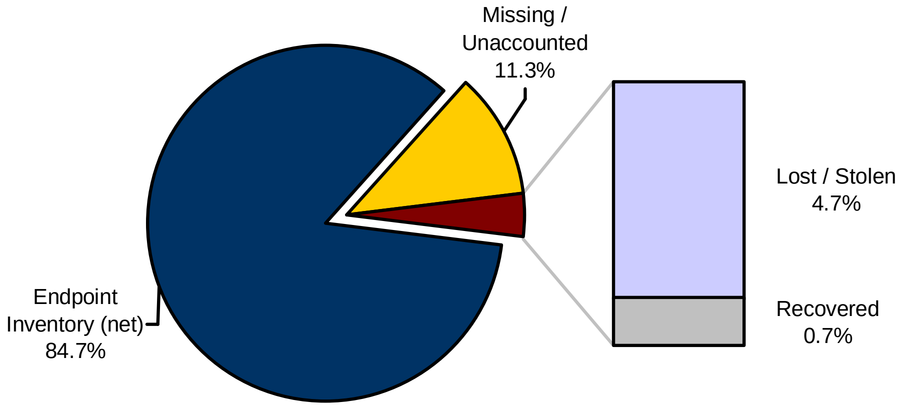
Does anyone remember the nursery rhyme and children's song about the five little ducks?

Five little ducks went out one day
Over the hill and far away
The mother duck said, "Quack, quack, quack, quack!"
But only four little ducks came back.

This little verse aptly describes how it is with enterprise endpoint systems, a term used here to refer generally to end-user computing platforms (e.g., personal computers, workstations, laptops, notebooks, netbooks) and the associated network connectivity, applications and data on which the enterprise end-users depend to carry out their daily tasks. In Aberdeen's study of over 150 organizations, for every 100 endpoints that went out only 85 endpoints came back (Figure 1), in spite of all the quacking.

Eleven are **missing and unaccounted** for – some perhaps are in the filing cabinet of the IT administrator, who hopes eventually to find time to re-image, re-install and re-provision them to new hires; some may be pressed into service in the home test lab of the field systems engineer; still others might never have been recovered from employees when they ended their employment. Five have been **lost or stolen** – not really a surprise, given that three out of five enterprise endpoints in the current study are regularly used for remote access to corporate systems. Of these five lost or stolen, only one is **successfully recovered** – unlike the happy ending in the nursery rhyme, in which "all of the five little ducks came back."

Figure 1: Where Have All the Enterprise Endpoints Gone?



Source: Aberdeen Group, February 2010

Fast Facts

Average time **endpoint management** initiatives have been in place:

√ Best-in-Class 4.6 years

√ Industry Average 3.1 years

√ Laggards 2.1 years

Average time **endpoint tracking and recovery** initiatives have been in place:

√ Best-in-Class 4.4 years

√ Industry Average 3.9 years

√ Laggards 3.7 years

Average time **endpoint anti-theft / deterrence** initiatives have been in place:

√ Best-in-Class 4.1 years

√ Industry Average 3.2 years

√ Laggards 2.9 years

The enterprises in Aberdeen's study have deployed an average of 13,900 endpoints at an average cost of $2,330. In **asset value** alone, the 15% net loss from lost, stolen and missing endpoints translates to a cost leakage of nearly $5M per year, not to mention the **inconvenience** and **opportunity cost** for affected end-users and administrators. Moreover, the potential impact of **data loss or data exposure** due to these lost, stolen or missing endpoints is an order of magnitude higher still – an average of $640,000 per incident based on Aberdeen's research, a figure which is modest in comparison to a number of other third-party studies. For so many topics in IT Security, it is typically either the law (i.e., *regulatory compliance*) or the lawless (i.e., *vulnerabilities and threats* derived from malicious intent) that demand our attention, but in the case of protecting and managing endpoints it is – or should be – viewed as a material *monetary* matter as well.

What to Do When it Happens to You: Five Questions

During the seven-year period between January 2003 and December 2009, public disclosures of data loss or data exposure due to computer-related loss, theft or disposal averaged more than three incidents per week and affected more than 150 million records, as summarized and catalogued on *www.datalossdb.org*. When the lost or stolen laptop happens to you – and the chances are extremely good that it will – there are five key questions to ask and answer:

1. **What happened?** Is it lost? Stolen? Missing? Were established policies and best practices followed?
2. **What assets are at risk?** Do we have accurate knowledge about the platform, software licenses, access to corporate networks and applications, and data – not only the end-user's working files, but also potentially sensitive information?
3. **What protections were in place?** Was the system and data backed up? Was the sensitive information encrypted? Can we remotely destroy or "wipe" the data? Can we remotely disable or "kill" the platform?
4. **Where is it now?** Can it be tracked? Can it be recovered? Do we know how to coordinate with appropriate law enforcement agencies?
5. **Can we prevent future occurrences?** What steps can be taken for deterrence of future loss, theft, or inventory "drift"?

Relative Importance Placed on the Five Questions

The relative importance that respondents place on the "Five Questions" and other aspects of protecting and managing their endpoint systems are summarized in Table 1, on a scale of 1 (lowest) to 5 (highest). **Having safeguards in place** ranked the highest, followed closely by establishing, communicating and enforcing **consistent policies and best practices** related to endpoints and having **accurate knowledge of what assets are at risk**. Reducing the actual number of lost, stolen or missing endpoints, and increasing the number of successfully recovered endpoints, ranked lower on the list. Given the high-level analysis discussed above, Aberdeen's research makes clear that companies have prioritized their investments based on a rational assessment of the greatest risks and on avoiding the greatest potential financial impact – and also that there are significant opportunities to reduce risk and save cost still on the table.

Table 1: Importance Placed on Selected Aspects of Protecting and Managing Endpoints

Ranking of Importance (1=Lowest, 5=Highest)	All Respondents	Relation to "5 Questions"
Having safeguards in place in the event of lost or stolen endpoints (e.g., encryption, data backup and recovery, remote "wipe" or "kill")	4.01	3
Establishing, communicating and enforcing consistent policies and best practices related to endpoints	3.75	1, 5
Accurate knowledge of what assets are at risk from lost or stolen endpoints (e.g., systems / platforms, software licenses, sensitive information)	3.73	2
Increased end-user productivity	3.67	-
Reduced operational costs	3.49	-
Reduction in the number of lost endpoints (e.g., inadvertent loss)	3.46	5
Improved regulatory compliance	3.44	-
Reduction in the number of stolen endpoints (e.g., criminal theft, opportunistic smash-and-grab)	3.27	5
Tracking and location of endpoint assets	3.18	4
Increase in the number of successfully recovered endpoints	3.11	4
Reduction in the number of missing endpoints (e.g., due to inventory "drift")	3.08	2

Source: Aberdeen Group, February 2010

Of notably *low* importance were aspects of **green and sustainability** initiatives related to endpoints, e.g., responsible eWaste disposal (2.68), provisioning of eco-friendly assets (2.49), and remote power management (2.43). While these activities are laudable in their own right, the findings are clear that in today's economic climate they are taking a back seat to other matters with higher risks and greater impact on costs.

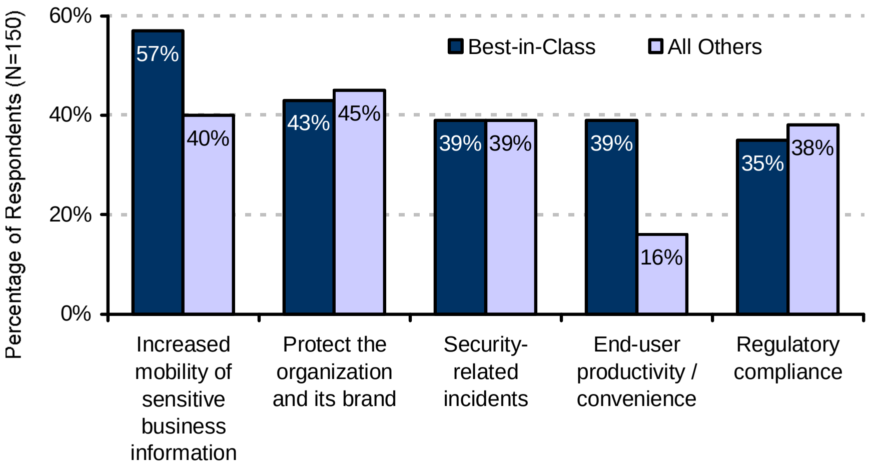
Market Drivers and Inhibitors

Risk is entrenched as the leading driver of current investments in protecting and managing enterprise endpoints, based on the *increased mobility of sensitive business information*, concerns about protecting the organization's *reputation and brand*, and actual *incidents of lost or stolen laptops* (Figure 2). For the leading performers, **end-user productivity and convenience** is also a top driver, by a factor of about 2.5-times in comparison to all other respondents. **Regulatory compliance**, encompassing both government and industry regulations, rounds out the list of motivators for current investments.

"Increasing insurance costs led us to improve our security situation as well as the more important task of preventing the loss of critical data to crime syndicates. The highest risk we have is reputational. A bank that is seen to not apply the highest standards to the security of personal data quickly loses the trust of its clients to handle their money."

~ Alan Britton, Group Programme Manager - Protection of Personal Information, Nedbank

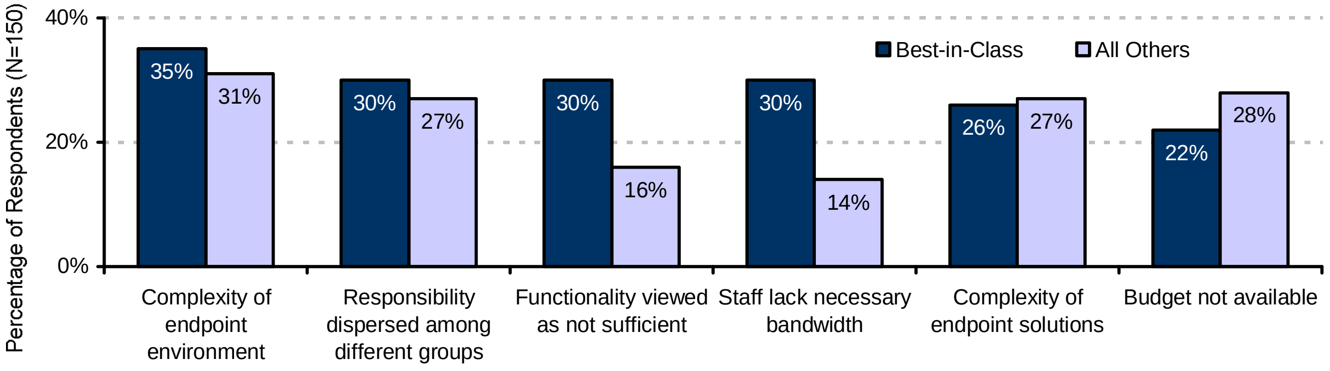
Figure 2: Top Drivers of Current Endpoint Investments



Up to three responses were accepted; does not add up to 100%
Source: Aberdeen Group, February 2010

Complexity is a leading *inhibitor* of current investments in protecting and managing enterprise endpoints, both in terms of the *complexity of existing endpoint environments* and of perceptions about the *complexity of currently available endpoint solutions* (Figure 3). **Resource limitations** (e.g., staff bandwidth, ambiguous accountability, available budget, and priority relative to other initiatives) and perceived **solution limitations** (e.g., desired functionality, ease of use) also contribute to inhibit current investments.

Figure 3: Leading Inhibitors to Current Endpoint Investments



Up to three responses were accepted; does not add up to 100%
Source: Aberdeen Group, February 2010

Maturity Class Framework: Defining the Best-in-Class

To distinguish Best-in-Class companies from Industry Average and Laggard organizations, Aberdeen used the year-over-year changes in the following performance criteria as they relate to protecting and managing endpoint systems:

- Number of actual security-related incidents (e.g., data loss or exposure, endpoint loss or theft)
- Number of non-compliance incidents (e.g., audit deficiencies)
- Number of help desk calls

The first two criteria were selected as measures of an organization's performance in managing risk and compliance, while the third was selected as an indicator of both cost and end-user convenience. Companies with top performance based on these criteria earned Best-in-Class status, as described in Table 2. (For additional details on the Aberdeen Maturity Class Framework, see Table 9 in Appendix A.)

Table 2: Top Performers Earn Best-in-Class Status

Definition of Maturity Class	Mean Class Performance (year-over-year change)
Best-in-Class: Top 20% of aggregate performance scorers	▪ **0.5% decrease** in the number of actual security-related incidents related to endpoints (e.g., data loss or exposure, endpoint loss or theft) ▪ **8.9% decrease** in the number of non-compliance incidents related to endpoints (e.g., audit deficiencies) ▪ **1.7% decrease** in the number of help desk calls related to endpoints
Industry Average: Middle 50% of aggregate performance scorers	▪ **1.0% increase** in the number of actual security-related incidents related to endpoints ▪ **1.2% increase** in the number of non-compliance incidents related to endpoints ▪ **2.3% increase** in the number of help desk calls related to endpoints
Laggards: Bottom 30% of aggregate performance scorers	▪ **10.7% increase** in the number of actual security-related incidents related to endpoints ▪ **9.6% increase** in the number of non-compliance incidents related to endpoints ▪ **10.0% increase** in the number of help desk calls related to endpoints

Source: Aberdeen Group, February 2010

The Best-in-Class PACE Model

Protecting and managing endpoint systems 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 8 in Appendix A). The characteristics exhibited by the Best-in-Class organizations in this study are summarized in Table 3.

Table 3: Best-in-Class PACE Framework for Protecting and Managing Endpoints

Pressures	Actions	Capabilities	Enablers (% of Best-in-Class adoption)
▪ Increased mobility of sensitive business information ▪ Protect the organization and its brand	▪ Sustain ongoing security and compliance requirements ▪ Establish and enforce consistent policies ▪ Educate end-users about policies and best practices ▪ Strive towards common endpoint security and endpoint management solutions ▪ Reduce the total cost of protecting and managing endpoints	▪ Consistent policies for supported endpoint access methods; for network access based on endpoint context; for supported endpoint software and licenses; for protecting sensitive data in use at the endpoints ▪ Systematic implementation and rollout processes for endpoint software, updates and configurations ▪ Responsible executive or team with primary ownership for security, compliance and management of endpoint systems ▪ Formal documentation, awareness and end-user training programs related to endpoints ▪ Discovery, classification, tracking and reporting of information assets ▪ Inventory, tracking and reporting of endpoint systems ▪ Standardized endpoint devices, platforms and configurations ▪ Technical controls to lock down standard configurations ▪ Visibility into current state / posture of endpoint systems under management ▪ Consistent, unified view of information and events related to endpoints ▪ Regular review and analysis of data from endpoint security and endpoint management systems	▪ Asset management (70%) ▪ Physical device security (65%) ▪ Asset tracking and recovery (48%) ▪ Remote disablement / kill (36%) ▪ Anti-Theft technology (26%) ▪ Trusted Platform Modules (22%) ▪ Authentication to device via password or PIN (96%), digital certificate (43%), biometric (17%) ▪ Online backup and recovery (file-based) (68%) ▪ Online backup and recovery (image-based / "bare metal") (50%) ▪ Data Loss Prevention (55%) ▪ Full-Disk Encryption (52%) ▪ File / Folder Encryption (48%) ▪ Remote destruction / "wiping" of data (27%)

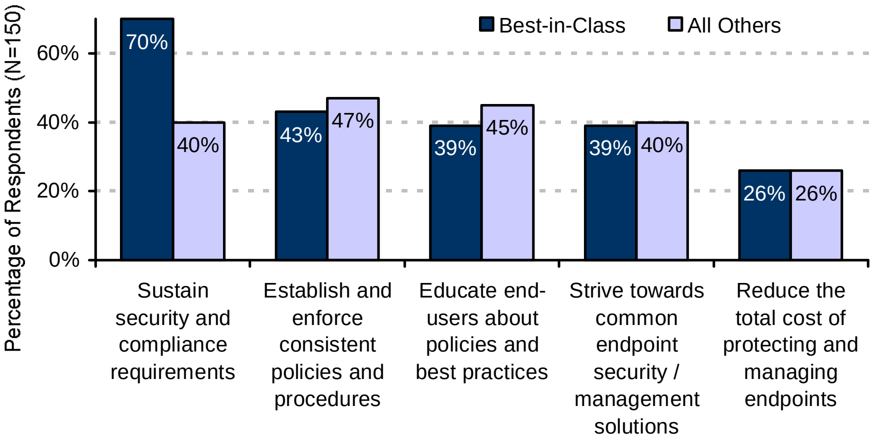
Source: Aberdeen Group, February 2010

Best-in-Class Strategies and Results

Sustaining requirements for **security** and **compliance** (both external regulations, and internal policies and procedures) is the leading strategy driving current investments in protecting and managing enterprise endpoints (Figure 4). With respect to compliance, the leading performers are nearly 6-times more likely than lagging performers to be focused on *sustaining* compliance than on *achieving* compliance, a clear indicator not only of the relative maturity of the Best-in-Class but also of the sheer complexity of the current compliance landscape. **Educating end-users** about endpoint-related policies and best practices is also a top strategy, for all respondents in the study. Companies are also looking to increase efficiencies, by **striving towards common solutions** for endpoint security and endpoint management, and by an explicit focus on **reducing the total cost** of protecting and managing the endpoints.

As an example of the latter, Aberdeen's benchmark study *Full-Disk Encryption On the Rise* (September 2009) showed that faced with a choice between the precision of encrypting only specific files or folders based on content and pre-existing policies, or the simplicity of encrypting everything on the hard drive, simplicity is increasingly favored over precision among those companies achieving Best-in-Class results. In a follow-on analysis of file / folder encryption users and full-disk encryption users (see *Endpoint Encryption Head to Head: File / Folder vs. Full-Disk*, January 2010), Aberdeen quantified the advantages of full-disk encryption in terms of greater security (cost avoidance) and lower total cost of ownership (cost savings).

Figure 4: Top Strategies Driving Current Endpoint Investments



Up to three responses were accepted; does not add up to 100%
Source: Aberdeen Group, February 2010

In the current study, what advantage do the top performers actually realize from their performance in endpoint tracking, recovery and deterrence? Table 4 presents a simple analysis of the Best-in-Class companies as compared to all other respondents, which indicates a cost savings of **$44 per endpoint**. Obviously this figure grows more meaningful for organizations with larger numbers of endpoints; for the participants in this study, this Best-in-Class advantage translates to an average cost savings of nearly **$800,000 per year**. At the same time, a significant opportunity for additional cost savings remains on the table: more than **$300 per endpoint** from further reductions in the net number of its endpoints that go lost, stolen or missing.

Table 4: Benefits of Endpoint Tracking, Recovery and Deterrence

Benefits of Tracking, Recovery and Deterrence	Best-in-Class	All Others	Best-in-Class Advantage
Endpoint Inventory (initial)	100.0%	100.0%	-
Less Unaccounted for	-10.3%	-11.5%	1.2%
Less Lost or Stolen	-4.2%	-4.8%	0.6%
Successfully Recovered after Lost or Stolen	*17.5%*	*14.5%*	*3.0%*
Plus Successfully Recovered	0.7%	0.7%	-
Endpoint Inventory (net)	86.2%	84.4%	1.8%
Endpoint Inventory Lost, Stolen, or Missing (net)	13.8%	15.6%	
Average Total Cost per Endpoint	$2,320	$2,330	-
Average Impact of Tracking and Recovery per Endpoint	$319	$363	**$44**
Average Number of Endpoints Deployed	18,100	13,100	38%
Cost Savings from Tracking, Recovery and Deterrence			**$795,000**

Source: Aberdeen Group, February 2010

It's worth repeating that although cost *savings* are more concrete, study participants tend to prioritize their investments based on cost *avoidance* from the potential loss or exposure of their sensitive data. Table 5 presents an analysis[1] of the advantage that Best-in-Class companies have in this regard, as a result of their implementation of endpoint protections such as remote wipe / disable and full-disk encryption. In this case, Best-in-Class performance translates to avoiding **more than 350 incidents** of potential data loss or data exposure. Based on previous Aberdeen research findings of $640,000 per incident – which is conservative compared to other industry estimates – top performance in implementing endpoint protections equates to tens of millions of dollars in potential costs avoided.

[1] This is a simplified analysis, ignoring the window of vulnerability between the point of loss or theft and the actual time of successful wiping or disablement, and also ignoring any overlap between the use of encryption and the use of remote wipe / kill. Although the latter scenario may seem like overkill to some, many companies are undoubtedly like the citizens of Munchkin City in *The Wizard of Oz*, who want the county Coroner to attest that their sensitive data is "not only merely dead, but really most sincerely dead."

Table 5: Benefits of Implementing Endpoint Protections

Benefits of Implementing Endpoint Protections	Best-in-Class	All Others	Best-in-Class Advantage
Lost or Stolen	4.2%	4.8%	0.6%
Successfully Wiped or Disabled after Lost or Stolen	*30%*	*12%*	*18%*
Successfully Wiped or Disabled	1.3%	0.6%	0.7%
Current Use of Full-Disk Encryption	*52%*	*32%*	*20%*
Protected by Encryption	2.2%	1.5%	0.7%
Average Number of Endpoints Deployed	18,100	13,100	38%
Incidents Avoided from Remote Wipe / Disable	228	74	**154**
Incidents Avoided from Full-Disk Encryption	397	199	**197**

Source: Aberdeen Group, February 2010

In the next chapter, we will see what the top performers are doing to achieve these gains.

Aberdeen Insights – Strategy

In Aberdeen's study of over 150 organizations, for every 100 enterprise endpoints that went out only 85 came back – 5 were lost or stolen, 1 of these was successfully recovered, and 11 are missing and unaccounted for. The research shows that companies currently prioritize their investments for protecting and managing endpoints in the following order:

- **Protecting against data loss or data exposure** – e.g., by encrypting sensitive information, by remotely destroying or "wiping" the data, or by remotely disabling or "killing" the platform. In doing so the top performers averted some 350 more potential incidents of data loss or data exposure over the last 12 months compared to all others, avoiding tens of millions of dollars of cost along as well as protecting their reputation and brand.
- **Minimizing disruption and opportunity cost to end-users and administrators** – e.g., by communicating consistent polices and best practices to end-users, by regularly backing up endpoint systems and data, and by implementing endpoint protection solutions with minimal impact on the end-user experience.
- **Reducing the number of endpoints that go lost, stolen or unaccounted for** – e.g., by maintaining accurate information about the company's platforms, software licenses and data, by the ability to track and recover when possible, and by deterring future occurrences. The cost savings realized by the top performers, in comparison to all others, was a non-trivial $44 per endpoint – and this still leaves more than $300 per endpoint in potential cost savings on the table as a future target.

Chapter Two: Benchmarking Requirements for Success

The selection of enabling technologies – along with the policy, planning, process, and organizational elements of implementation – are critical success factors in the ability for an enterprise to realize the business benefits of protecting and managing its endpoint systems.

Case Study –Australian Investment and Banking Company

A large Australian-based investment and banking company, founded over 150 years ago, uses laptop anti-theft, tracking and security solutions to protect their sensitive information and provide risk assurance to their stakeholders.

"The perceived safety of our information is a big deal for us," explained a senior manager in their Risk and Compliance Group. "Despite strong passive security measures, the lack of 'active' participation in the protection of our organization's assets was sounding some warning bells. We took a look at anti-theft and asset tracking solutions as a way to give us a more hands-on approach to information security, and to provide the means for people in the organization to have full accountability for their actions."

Remote intervention for lost or stolen laptops and ease of encryption were two of the main criteria this company established for selecting a security vendor. The rate of security incidents has dropped since the adoption of these solutions, and with the added functionality the company is now able to provide specific assurances to its risk committee and board members.

"Be clear about the value of your information and why it is important to protect it," advises the Risk and Compliance Group manager. "Information as a quantifiable asset is still a difficult concept for many executives. Continuous education on the real risks and costs of security incidents is required so that informed business decisions can be made."

Competitive Assessment

Aberdeen analyzed the aggregated metrics of surveyed companies to determine whether their performance in protecting and managing its endpoint systems ranked as Best-in-Class, Industry Average, or Laggard. In addition to having similar 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 business intelligence 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

Fast Facts

Percentage of enterprise endpoints used for **remote access** to corporate resources:

√ Best-in-Class 62%

√ Industry Average 62%

√ Laggards 43%

Percentage of enterprise endpoints tracked with respect to their **current location:**

√ Best-in-Class 54%

√ Industry Average 29%

√ Laggards 19%

Percentage of enterprise endpoints tracked with respect to **applications installed** and **software licenses in use:**

√ Best-in-Class 96%

√ Industry Average 77%

√ Laggards 50%

ability of the organization to measure results to improve the business). These characteristics, identified in Table 6, serve as a guideline for best practices, and correlate directly with Best-in-Class performance across the associated metrics.

Table 6: Competitive Framework for Endpoints

	Best-in-Class	Average	Laggards
Process	Consistent policies for supported endpoint access methods; for network access based on endpoint context; for supported endpoint software and licenses; for protecting sensitive data in use at the endpoints		
	83%/78%/78%/74%	62%/51%/38%/49%	57%/49%/37%/42%
	Systematic implementation and rollout processes for endpoint software, updates and configurations		
	74%	52%	48%
Organization	Responsible executive or team with primary ownership for security, compliance and management of endpoint systems		
	70%	54%	51%
	Formal documentation, awareness and end-user training programs related to endpoints		
	61%	50%	37%
Knowledge Management	Discovery, classification, tracking and reporting of data		
	61%	34%	26%
	Inventory, tracking and reporting of endpoint systems		
	57%	48%	26%
Technology	Standardized endpoint devices, platforms; Standardized configurations; Technical controls to lock down standard configurations		
	86% / 82% / 64%	59% / 53% / 45%	50% / 52% / 42%
	See **Table 6** for an illustrative list of enabling technologies commonly used in protecting and managing endpoint systems; see **Figure 10** for insights into the adoption of enabling technologies by Best-in-Class organizations.		
Performance Management	Visibility into current state / posture of endpoint systems under management		
	48%	29%	27%
	Consistent, unified view of information and events related to endpoints		
	43%	25%	24%
	Regular review and analysis of data from endpoint security and endpoint management systems		
	57%	32%	24%

Source: Aberdeen Group, February 2010

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 capabilities for protecting and managing endpoint systems beyond that of their Industry Average and Laggard counterparts.

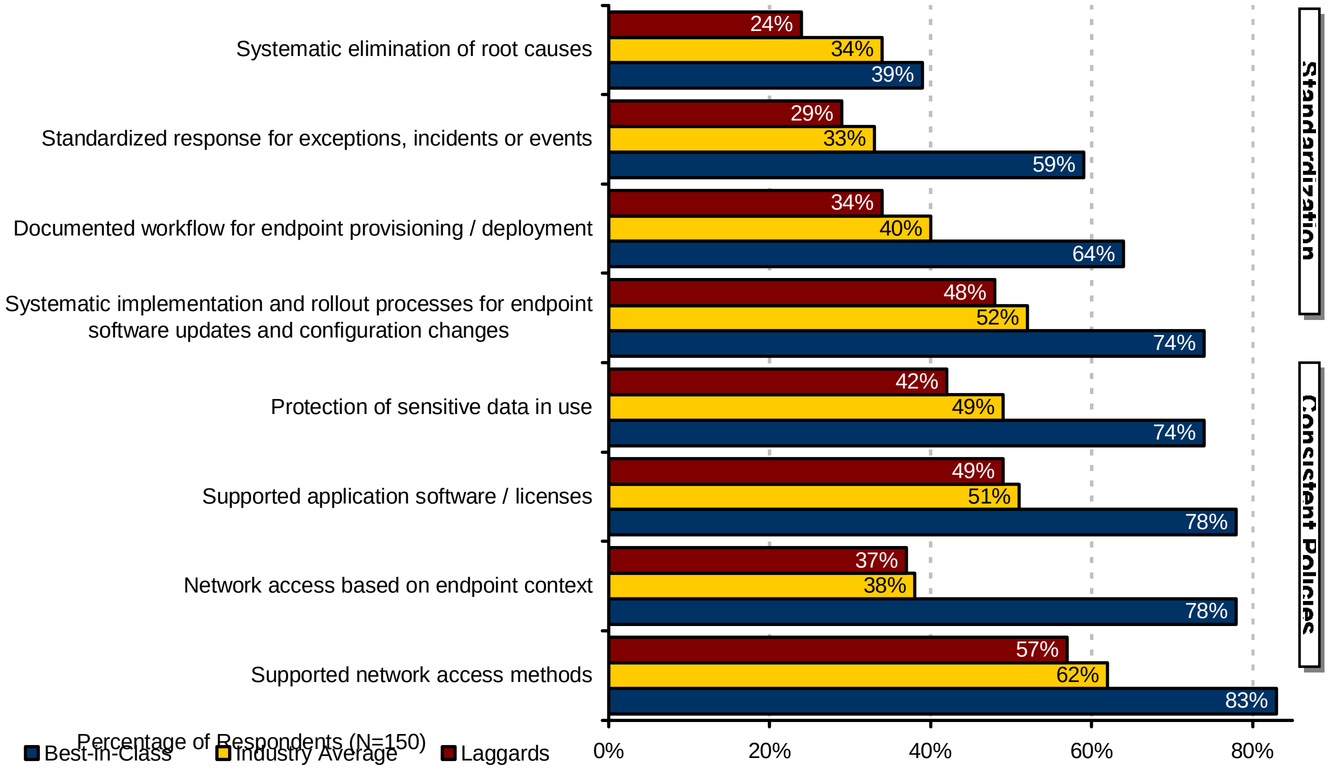
> "We made our anti-theft solution selection based on which product was being used by other universities, had a quick and easy deployment, was low cost, and had the capability for central administration by our campus police department."
>
> ~ D. Douglas Badger, Director of IT Portfolio Management & Systems Assurance, University of Guelph

Process

Consistent policies drive top results, as Aberdeen has observed in virtually every IT Security benchmark study (Figure 5). With respect to endpoints, this includes consistent policies for:

- Supported *network access methods* (e.g., wired, wireless, VPN, and Web)
- Network access based on *endpoint context* (e.g., configuration, "health", device identification, and user authentication to device)
- Supported *application software / licenses* (including acceptable employee-installed applications)
- *Backup and recovery* of endpoint data (e.g., file-based, image-based), and *explicit safeguards* for sensitive data (e.g., full-disk encryption)

Figure 5: Consistent Policies, Standardized Processes Drive Top Results



Source: Aberdeen Group, February 2010

In addition, top performance is strongly correlated with the **standardization of processes** across the entire endpoint lifecycle, including:

- *Roll out* (e.g., consistent workflow for endpoint provisioning and deployment)
- *Regular updates* (e.g., systematic implementation and rollout processes for endpoint software updates and configuration changes)
- *Incident response* (e.g., standardized response for endpoint-related exceptions, security events, or incidents of non-compliance)
- *Continuous improvement* (e.g., systematic elimination of root causes for endpoint-related exceptions, security events or incidents of non-compliance)

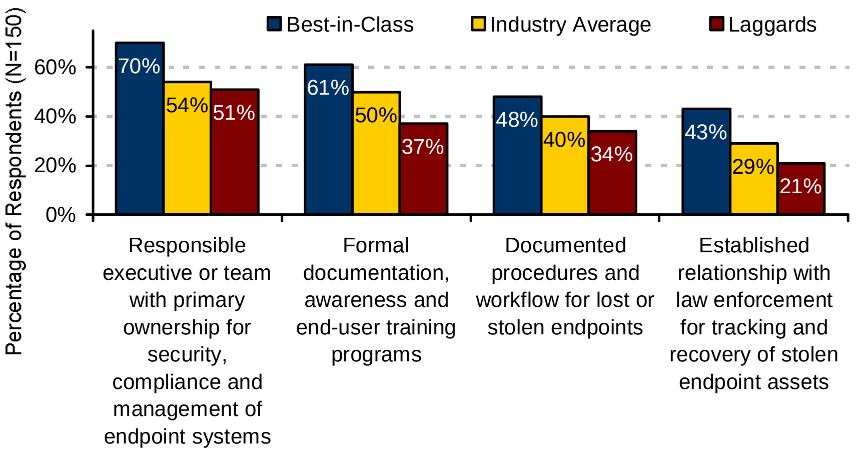
In musical terms, Best-in-Class companies operate like practiced, classical chamber music ensembles; Laggards operate like improvisational jazz combos, where the jazz is bad.

Organization

The top performers rely not on good intentions, but on **accountability** and **planning**. As found in virtually every Aberdeen IT Security benchmark study, having a responsible executive or team with primary ownership – the "*one throat to choke*" principle – is correlated with the achievement of Best-in-Class results (Figure 6). *Educated end-users*, through formal documentation, awareness and training programs related to endpoint policies, are another important aspect of accountability as carried out by Best-in-Class organizations. When lost or stolen endpoint scenarios do come to pass, the top performers rely on documented procedures and workflow, and on established relationships with law enforcement agencies for potential tracking and recovery.

> "Solid policy and end-user education are just as important as the technical solutions. Ditto for emergency response procedures, for when a loss or theft does occur."
>
> ~ Rick Riordan, Executive Vice President of Shared Services, CedarCrestone Inc.

Figure 6: Accountability and Planning

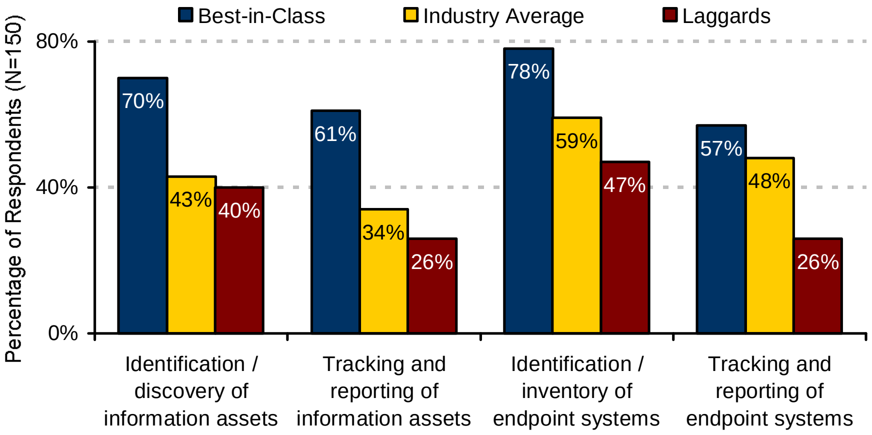


Source: Aberdeen Group, February 2010

Knowledge Management

Best-in-Class companies are more likely than their Industry Average and Laggard counterparts to **identify, track, and report on** the status of their endpoint-related assets over time – including endpoint *platforms*, *application software / licenses*, and *information assets* (Figure 7). Being able to answer the question "what assets are at risk" when endpoints are lost or stolen is one of the foundational elements for achieving top results.

Figure 7: Identification, Tracking and Reporting on Assets

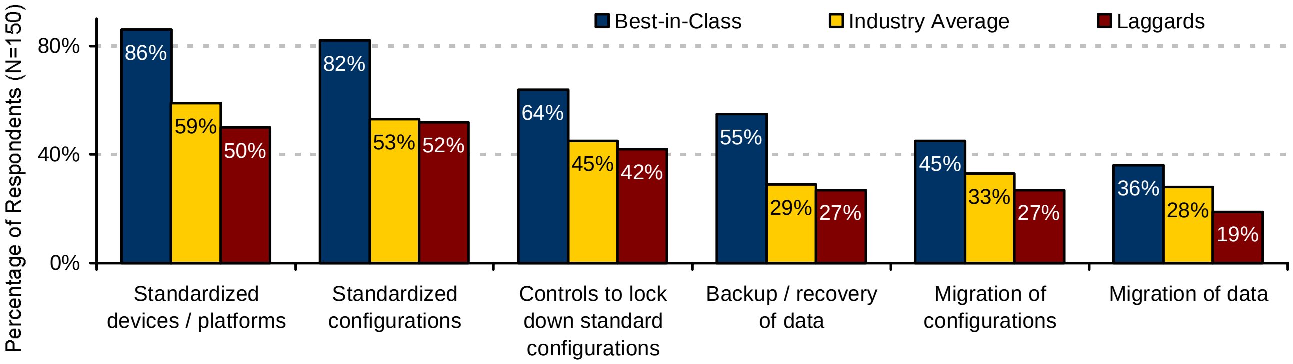


Source: Aberdeen Group, February 2010

Technology / Automation

For the top performers, the theme of standardization is also more likely to extend beyond policies and processes to include **standardization of endpoint devices and configurations**, the implementation of technical controls to lock them down, and the automated migration of configurations and data when endpoint systems need to be swapped out or replaced (Figure 8).

Figure 8: Standardization of Platforms and Configurations; Backup and Migration of Data



Source: Aberdeen Group, February 2010

This element of uniformity for laptops and notebooks is in stark contrast to the more liberal approach that Best-in-Class companies have adopted in their formal support for smart phones, USB drives and other "mobile" endpoint devices. The typical enterprise is already teeming with these types of devices, many of which are accessing corporate email, applications and data. No longer an exclusive perquisite of the executive ranks, the blended personal / professional use of this class of endpoints has become the "new normal" for enterprise end-users. Looking the other way, as end-users attempt to self-manage an array of unsupported devices, exposes the organization to a set of under-recognized security risks to its IT infrastructure and its critical applications and data. See Aberdeen's benchmark report *Going Mobile: Securing and Managing Smart Phones* (January 2010) for additional insights on key issues and best practices in this area.

But for laptops and notebooks, the research shows that the top performers are much more likely than all others to standardize and lock down their platforms and configurations, and to remotely disable or “kill” the platforms if they are lost or stolen. Similarly, the top performers are more likely to regularly back up and encrypt their endpoint data, and to remotely destroy or “wipe” the data if the endpoint is lost or stolen. To paraphrase Robert F. Kennedy, people may say that such practices are ruthless, but Best-in-Class companies are not ruthless … and if they find the people calling them ruthless, they will destroy them.

> “Whole-disk encryption is an inelegant, clumsy, brute force, and lazy solution for endpoint security … but necessary.”
>
> ~ Rick Riordan, Executive Vice President of Shared Services, CedarCrestone Inc.

Table 7: Enabling Technologies Commonly Used in Protecting and Managing Endpoint Systems

	Protect	Manage
Data	▪ **File / folder encryption** ▪ **Full-disk encryption** ▪ **Device / port controls** ▪ **Data loss prevention** ▪ USB drive encryption ▪ Email encryption	▪ **Online backup / recovery (file-based)** ▪ **Online backup / recovery (image-based)** ▪ **Remote destruction / “wiping” of data**
Applications	▪ Email monitoring / filtering ▪ Web monitoring / filtering	▪ Software distribution ▪ Software inventory / usage management ▪ Application virtualization
Networks	▪ Personal firewalls ▪ Intrusion detection / prevention ▪ Network access control	
Platforms	▪ Anti-virus / anti-malware ▪ Patch management ▪ Configuration / change management ▪ **Physical device security** ▪ **Anti-Theft technology**	▪ **Remote disablement / “kill” of endpoints** ▪ Patch management ▪ Configuration / change management ▪ **Asset management** ▪ **Asset tracking / recovery**

Source: Aberdeen Group, February 2010

Table 7 provides an illustrative (i.e., not intended to be comprehensive) list of enabling technologies which are commonly used in protecting and managing endpoint systems. The list is further categorized by the primary *focus* of these technologies, i.e., on **platforms**, **networks**, **applications**, or **data**. The technologies emphasized in bold type are those that are most relevant for the Five Questions and the thematic issue of lost, stolen or missing endpoints. While not necessarily exhaustive, the listing and organization of the endpoint security and endpoint management technologies as provided in Table 7 helps to extract several interesting insights when examining the trends in current use, as reported by the participants in the current study. For example, Figure 10 plots the research findings for *absolute adoption* by the Best-in-Class (i.e., the percentage of Best-in-Class organizations indicating current use) versus *relative adoption* by the Best-in-Class (i.e., the ratio of current use by Best-in-Class organizations to that of Laggards). See the "Aberdeen Insights" section on Technology at the end of this chapter for additional discussion.

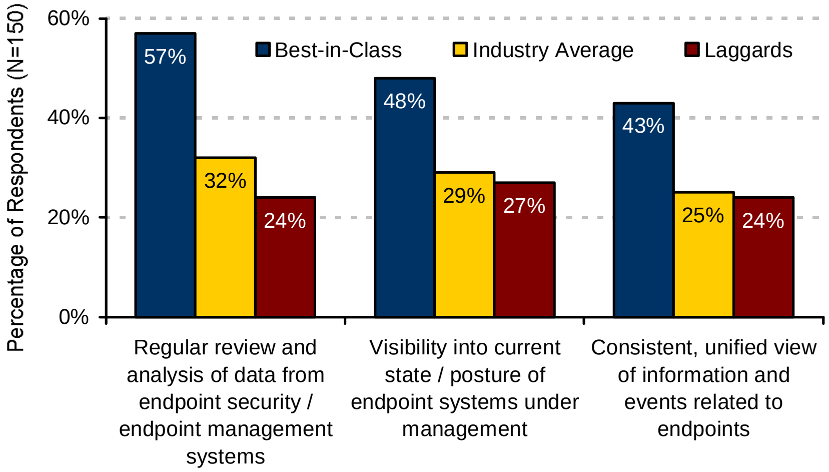
Performance Management

Finally, the leading performers are about 2-times more likely than lagging performers to actually **make use of the information that is available** from their endpoint security and endpoint management systems (Figure 9). They *regularly review and analyze* the data, they *maintain visibility* into the current state and posture of the endpoints under management, and they work to *establish a consistent, unified view* of information and events related to their endpoint systems. To paraphrase Thomas Paine, those who expect to reap the blessings of their endpoint systems must also undergo the fatigue of supporting them.

"Don't underestimate the importance of on-going care and feeding of these systems – they need dedicated skills and effort to manage and maintain."

~ Stephen Kish, IT Manager, City of Surrey

Figure 9: Making Use of Available Information

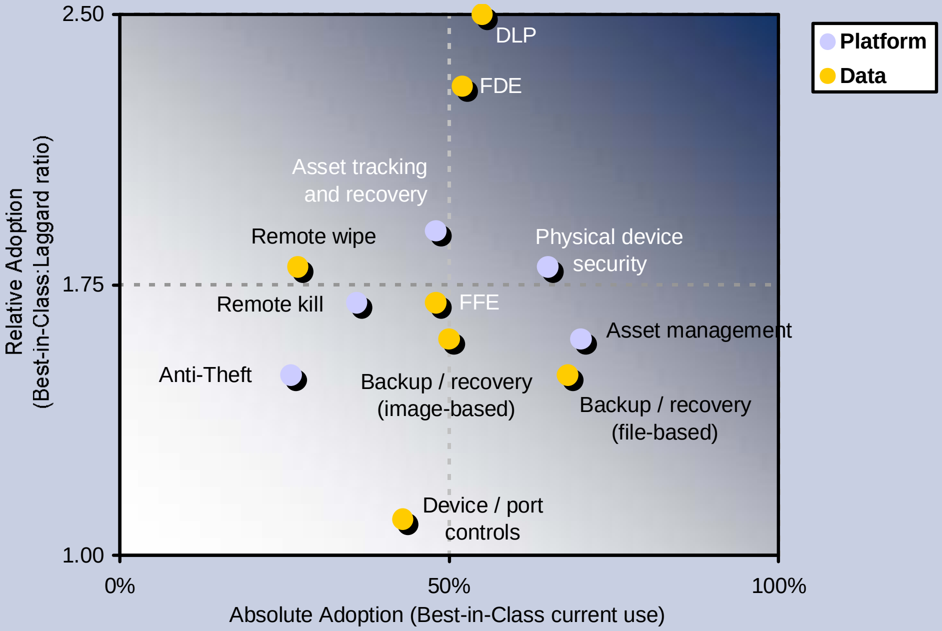


Source: Aberdeen Group, February 2010

Aberdeen Insights – Technology

Aberdeen's research findings regarding the enabling technologies used to protect endpoint **platforms** and **data** are summarized in Figure 10, which plots the *absolute adoption* by the Best-in-Class (i.e., the percentage of Best-in-Class organizations indicating current use) versus the *relative adoption* by the Best-in-Class (i.e., the ratio of current use by Best-in-Class organizations to that of Laggards). This scatter-gram presentation of the data naturally lends itself to interpretation as a simple 2-by-2 matrix, with four distinct quadrants.

Figure 10: Current Use of Enabling Technologies by the Best-in-Class



Source: Aberdeen Group, February 2010

The **platform**-oriented technologies in Figure 10 – *asset management*, *asset tracking and recovery*, *remote kill*, and *anti-theft* – have been adopted by the Best-in-Class to varying degrees, but all are more than 1.5-times more likely to have been adopted by the leading performers than by Laggards. For the participants in this study, *asset tracking and recovery* stands out as the enabling technology that most strongly differentiates Best-in-Class performance.

Similarly, the **data**-oriented technologies in Figure 10 – including *file-based* and *image-based backup and recovery*, *file / folder encryption*, *remote wipe*, *full-disk encryption*, and *Data Loss Prevention (DLP)* – are all more than 1.5-times more likely to have been adopted by the Best-in-Class than by Laggards, with *full-disk encryption* and *DLP* as the strongest differentiators of top performance. In general, these findings are consistent with the observation that companies have prioritized their investments to date based on a rational assessment of the greatest risks and on a desire to **avoid cost**, although investments designed to **save cost** are on the rise.

Chapter Three: Recommended Actions

Whether a company is trying to move its performance in protecting and managing its endpoint systems from Laggard to Industry Average, or Industry Average to Best-in-Class, the following actions will help to drive the necessary improvements – and serve to answer the five key questions that will be asked when a lost or stolen laptop inevitably happens:

1. What happened?
2. What assets are at risk?
3. What protections were in place?
4. Where is it now?
5. Can we prevent future occurrences?

Fast Facts

Year-over-year change in **total management costs** related to endpoints:

√ Best-in-Class 0.5% *decrease*

√ Industry Average 2.3% *increase*

√ Laggards 8.4% *increase*

Define and Manage What's Supposed to Happen

- **Establish consistent policies and procedures**, including:
  - Standardized endpoint devices, platforms and configurations
  - Systematic implementation and rollout processes for endpoint software, updates and configurations
  - Protections for sensitive data in use at the endpoints
- **Educate your end-users** with formal documentation, awareness and training about policies for managing and protecting endpoints.
- **Maintain current information** about your endpoint assets, by implementing the following capabilities:
  - Inventory, tracking and reporting of endpoint devices and platforms
  - Visibility into the current state / posture of endpoint systems under management
  - Discovery, classification, tracking and reporting of information assets at the endpoints
- **Manage endpoints proactively**:
  - Develop a consistent, unified view of information and events related to endpoints
  - Regularly review and analyze the data from endpoint security and endpoint management systems

"The major lesson we learned is that people cause the problems, not the technology. You have to tackle the people issues first, so they fully understand the reasons for certain software and hardware approaches."

~ Alan Britton, Group Programme Manager - Protection of Personal Information, Nedbank

Understand What Assets are at Risk

- **Maintain current information** about your endpoint assets, including devices / platforms, software licenses, and sensitive information. Enabling technologies for these capabilities include:

- *Asset management* (implemented by 70% of the Best-in-Class companies in this study)
- *Software inventory / usage management* (61%)
- *Asset tracking and recovery* (48%)
- *Online backup and recovery*, both file-based (68%) and image-based / "bare metal" (50%)
- *Data Loss Prevention* (55%)

Put Appropriate Protections in Place

- **Protect the data**, by using enabling technologies that include:
  - *Online backup and recovery*, either *file-based* (implemented by 68% of the top performers) or *image-based / "bare metal"* (50%). Aberdeen's research shows that file-based backup and recovery is more widely deployed, but Best-in-Class companies are more strongly differentiated by the use of image-based solutions.
  - *Encryption*, both *full-disk* (52%) and *file / folder* (48%). Both approaches are widely deployed, but Aberdeen's research over the last two years makes it clear that full-disk encryption is on the rise due to the simplicity of encrypting everything on the endpoint.
  - *Remote destruction / "wiping"* of data (27%).
- **Protect the endpoint device / platform**, by using enabling technologies that include:
  - *Authentication* to the device, most commonly using simple *passwords or PINs* (implemented by 96% of the Best-in-Class), but also using stronger authentication methods such as *digital certificates* (43%) and *biometrics* (17%).
  - *Remote disablement / "kill"* capabilities (36%), which effectively transforms the platform into a brick.

Track and Recover Endpoint Assets

- **Assess the opportunity** to reduce the 15% net loss from lost, stolen and missing endpoints, which translates to a cost leakage of nearly $5M per year for the average respondent in this study – not to mention the inconvenience and opportunity cost for affected end-users and administrators. Enabling technologies include *asset tracking and recovery* (implemented by 48% of the top performers), and best practices include establishing working relationships with the appropriate law enforcement agencies (43%). Although the top performers realize a $44 per endpoint cost savings compared to all others in the study, an opportunity of more than $300 per endpoint remains as a target based on additional reductions in the net number of lost, stolen and missing endpoints.

Prevent Future Occurrences

- **Deterrence** is best achieved by improving adherence to established policies and best practices, as described above in "defining and managing what's supposed to happen." The use of hardware-based *anti-theft technologies* (implemented by 26% of the Best-in-Class companies in this study) is also increasing in popularity, based on their ability to disable lost or stolen endpoints both with and without a network connection. These solutions are also capable of disabling the platform automatically based on the detection of suspicious behavior (e.g., excessive login attempts, failure to check in within a prescribed period of time) and to re-enable platforms quickly upon recovery.

Aberdeen Insights – Summary

When the lost or stolen laptop happens to you – and the chances are extremely good that it will – there are five key questions to ask and answer: What happened? What assets are at risk? What protections were in place? Where is it now? Can we prevent future occurrences? Compared to all others in the study, the top performers realize $44 per endpoint in *cost savings* from reducing the net number of lost, stolen and missing endpoints, and tens of millions of dollars in *costs avoided* by averting more than 2-times the number of data loss or data exposure incidents. Aberdeen's research shows that best practice as established by the Best-in-Class organizations is to:

- **Protect against data loss or data exposure**, by encrypting sensitive information, by remotely destroying or "wiping" the data, or by remotely disabling or "killing" the platform.
- **Minimize disruption and opportunity cost to end-users and administrators**, by communicating consistent polices and best practices, by regularly backing up endpoint systems and data, and by implementing endpoint protection solutions with minimal impact on the end-user experience.
- **Reduce the number of endpoints that go lost, stolen or unaccounted for**, by maintaining accurate information about the company's platforms, software licenses and data, by the ability to track and recover endpoints when possible, and by taking proactive steps to deter future occurrences.

Appendix A: Research Methodology

Between January and February 2010, Aberdeen examined the use, the experiences and the intentions of more than 150 enterprises from a diverse set of industries with respect to their approach to protecting and managing their endpoint systems. Aberdeen supplemented this online survey effort with interviews with select survey respondents, gathering additional information on their respective strategies, experiences and results.

Responding enterprises had the following demographics:

- *Job title / function:* The research sample included respondents with the following job titles: C-level management (16%); Vice President / General Manager (10%); Director (22%); Manager (32%); Staff / Consultant (19%); and Other (1%). The largest segment by functional responsibility was IT, representing 53% of the total sample.
- *Industry:* The research sample included respondents from a wide range of industries. The largest segments included government / aerospace / defense (11%); financial services (15%); telecommunications (11%); education (10%).
- *Geography:* The majority of respondents (62%) were from the Americas. Remaining respondents were from Europe / Middle East / Africa (29%) and the Asia / Pacific region (9%).
- *Company size:* Twenty-seven percent (27%) of respondents were from large enterprises (annual revenues greater than US $1 billion); 32% were from mid-size enterprises (annual revenues between $50 million and $1 billion); and 41% were from small businesses (annual revenues of $50 million or less).

Focus of the Study

Respondents completed an online survey that included questions designed to determine the following:

√ The degree to which endpoint security and endpoint management are currently deployed, and the financial implications of their use

√ The efficiency and effectiveness of existing implementations

√ Benefits that have been derived with respect to enhancing security, sustaining compliance, managing risk, and reducing cost

The study aimed to identify current and emerging best practices for protecting and managing endpoints, and to provide a framework by which readers can assess their own current capabilities.

Table 8: PACE Framework Key

Overview
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 (e.g., economic, political and regulatory, technology, changing customer preferences, competitive) **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) **Capabilities –** the business process competencies required to execute corporate strategy (e.g., skilled people, brand, market positioning, viable products / services, ecosystem partners, financing) **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)

Source: Aberdeen Group, February 2010

Table 9: Competitive Framework Key

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

Source: Aberdeen Group, February 2010

Table 10: Relationship Between PACE and the Competitive Framework

PACE and the Competitive Framework – How They Interact
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.

Source: Aberdeen Group, February 2010

Appendix B:
Related Aberdeen Research

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

- *Going Mobile: Securing and Managing Smart Phones, USB Drives and Other Mobile Endpoint Devices;* January 2010
- *IT Security: Balancing Enterprise Risk and Reward*; January 2010
- *Endpoint Encryption Head-to-Head: File / Folder vs. Full-Disk*; January 2010
- *Priorities in IT Asset Disposal: Data Protection vs. Environmental Compliance*; November 2009
- *Why DLP Users Don't Discover Data*; November 2009
- *Full-Disk Encryption On the Rise*; September 2009
- *File Transfer is Not What it Used to Be: It's Secure, Reliable and Well-Managed*; July 2009
- *Securing Unstructured Data: How Best-in-Class Companies Manage to Serve and Protect*; June 2009
- *The Cost-Based Business Case for DLP*; June 2009
- *Endpoint Security, Endpoint Management: The Cost-Cutter's Case for Convergence*; March 2009
- *Managing Encryption: The Keys to Your Success*; October 2008
- *Data Loss Prevention: Little Leaks Sink the Ship*; June 2008
- *Protecting Data at the Endpoints: Combating Lost/Stolen Laptops, Thumb-Sucking, Pod-Slurping, and Other Threats to Your Sensitive Data* ; December 2007

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

Authors: Derek E. Brink, Vice President and Research Fellow, IT Security, (Derek.Brink@aberdeen.com);
Nathaniel Rowe, Research Associate (Nathaniel.Rowe@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.

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. Solution providers recognized as underwriters 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.

Absolute® Software is the world leader in tracking, managing and protecting digital assets for better data protection, easier computer lifecycle management and managed computer theft recovery. With our Computrace®, Absolute Manage™ and Computrace® LoJack® for Laptops™ solutions, large enterprises, small businesses and individuals can protect and manage their computing devices and data.

Absolute solutions help you track and control your IT assets, reduce costs and deter theft. Plus, you can remotely delete data, get the device back and prove data was not accessed – helping you avoid costly regulatory fines as well as damage to your reputation and brand.

For additional information on Absolute Software:

Stephen Midgley
1600-1055 Dunsmuir Street
Vancouver, BC, V7X 1K8
Telephone: 1- (604) 730-9851
www.absolute.com
info@absolute.com

Intel, the world leader in silicon innovation, develops technologies, products and initiatives to continually advance how people work and live.

Intel® Anti-Theft Technology, available on select all-new 2010 Intel® Core™ processor family-based laptops, frustrates thieves by locking access to a PC if a central server or built-in intelligence concludes it is lost or stolen. New Intel Anti-Theft Technology version 2.0 (Intel® AT 2.0) enables encryption solutions to disable access to cryptographic keys through hardware to completely block access to data, and also makes it simpler to reactivate a PC once in rightful hands. Also, a custom message can be displayed in a pre-OS screen of the disabled PC for anyone who tries to access the computer.

For additional information on Intel:

Danielle Galbraith
2200 Mission College Blvd.
Santa Clara, CA 95054-1549
Telephone: (408) 765-8080
www.intel.com
danielle.galbraith@intel.com

WinMagic is a worldwide leader in developing disk encryption software. WinMagic's SecureDoc protects sensitive data stored on laptops, workstations and removable media including USB thumb drives and CD/DVDs. Thousands of the most security conscious enterprises and government organizations around the world depend on SecureDoc to minimize business risks, meet privacy and regulatory compliance requirements, and protect valuable information assets against unauthorized access. With a full complement of professional and customer services, WinMagic supports over three million SecureDoc users in approximately 43 countries.

For additional information on WinMagic:

Joseph Belsanti
200 Matheson Blvd. West, Suite 201
Mississauga, ON, L5R 3L7
Canada
Telephone: +1-(905) 502-7000
Toll-Free: 1-(888) 879-5879
www.winmagic.com
info@winmagic.com