Aberdeen Group
A Harte-Hanks Company

# Full-Disk Encryption

On the Rise

September 2009

Derek Brink

# Executive Summary

The simplicity of encrypting everything on the endpoint, or the precision of encrypting only specific files or folders based on content and pre-existing policies? 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.

## Best-in-Class Performance

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

- Number of security incidents (e.g., data loss or data exposure)
- Number of non-compliance incidents (e.g., audit deficiencies) related to endpoint encryption
- Amount of human error (e.g., policy violations)

In addition, Aberdeen used the number of intentional data loss or data exposure incidents from internal sources (e.g., non-malicious violations of policy by well-intentioned end-users trying to carry out their everyday tasks) experienced over the last 12 months. 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 in endpoint encryption shared several common characteristics, including:

- 41% discover all information assets; 56% classify information by requirements for confidentiality, integrity and availability
- 44% have systematic implementation / rollout processes for encryption solutions
- 62% have a responsible executive or team with primary ownership for endpoint encryption initiatives
- 50% provide awareness and training programs for end-users
- 41% automatically enforce data protection policies (transparent to end-users)
- 58% have centralized management of configurations and policies; 41% have centralized management of the encryption key lifecycle

## Recommended Actions

In addition to the specific recommendations in Chapter Three, to achieve Best-in-Class performance in endpoint encryption companies should strive to be secure first, then compliant; stated another way, they should adopt a risk-based – as opposed to a regulation-based – approach to IT Security.

### Research Benchmark

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

"In the evaluation of file / folder encryption versus full-disk encryption, our leading consideration was that encryption not be based on end-user decisions. Solutions that can base the encryption based on policies we set for the user, such that the data defined as encrypted for that user will *be* encrypted whether the user knows it or not, are very compelling for larger organizations needing to perform centralized management on endpoint computers. We are currently examining the impact on our operations between two products, in terms of greatest flexibility and least impact."

~ IT Staff Member,
US State Government Agency

## Table of Contents

## Figures

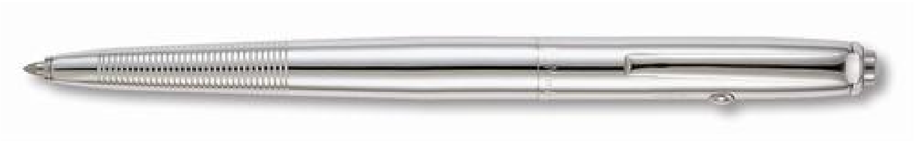
## Tables

# Chapter One: Benchmarking the Best-in-Class

## Business Context: Space Pens and Ballistic Missiles

The story is apocryphal as it is commonly told[1], but no less instructive: in the Space Race between the Soviet Union and the United States in the 1960s, cosmonauts and astronauts needed a writing instrument that would work in a vacuum, in zero gravity, and in the temperature extremes of hot sunlight and cold shadow. At great expense, the Americans developed a high-tech, pressurized ball point pen – the "Space Pen" – that met these requirements. The Soviet solution: a standard graphite pencil.

### Figure 1: AG7, The Original Astronaut Space Pen



Source: Fisher Spacepen Company, www.spacepen.com

A story from the latter part of the Cold War provides a similar lesson: the design of Intercontinental Ballistic Missiles (ICBMs), designed to carry nuclear warheads from launch positions in one superpower to designated targets in another. By the early 1980s, American missiles were engineered to be small, efficient, and precise in terms of both accuracy and time-on-target. Soviet missiles were larger, less efficient and less accurate, which fostered a different approach to success: bigger bombs. What they lacked in precision, they made up for in megatons.

In many ways, these two examples parallel the IT decisions that today's enterprises are making with respect to the deployment of **encryption** to protect sensitive data on their endpoint systems. **File / folder encryption** is more precise, encrypting only specific files or folders based on the content and the pre-existing policies. Success of file / folder encryption initiatives requires that consistent policies regarding what data should be encrypted are firmly in place, and that they can be carried out efficiently and

Fast Facts

Average time an endpoint encryption initiative has been in place:

√ Best-in-Class: 3.5 years

√ Industry Average: 2.9 years

√ Laggards: 2.3 years

Definitions

For the purposes of this study:

√ **File / folder encryption** refers to the transformation (*encryption*) of information in specific files or folders into a form that cannot be read without the possession of special knowledge, referred to as a *key*.

√ **Full-disk encryption** refers to encryption of the entire hard drive. As with file / folder encryption, the objective is to ensure that the information being protected remains private from anyone not authorized to read it, even from those who may have access to the encrypted data itself.

√ **Endpoint** or **endpoint system** refers generally to end-user computing platforms (e.g., personal computers, workstations, laptops, notebooks, netbooks) and the associated applications, data, and network connectivity on which the end-users depend.

[1] The more accurate history is that at the beginning of their respective space programs, both cosmonauts and astronauts used lead pencils. Their tips sometimes broke off, however, and became floating, flammable safety hazards in zero gravity outer space. Recognizing the need for an alternative, the Fisher Space Pen was developed independently by Paul Fisher, and after testing and approval by NASA for use in space the Americans replaced the pencil starting in 1968. Eventually both astronauts and cosmonauts used the Fisher Space Pen in place of the pencil.

reliably. **Full-Disk Encryption (FDE)**, by encrypting "everything" on the endpoint system, has less dependence on the precision of policies and the accuracy of enforcement. Success of full-disk encryption requires that solutions address issues of performance, integration, management and scale.

## *Ample Evidence of Risk of Data Loss or Data Exposure*

Awareness of the *need* for endpoint encryption can be found readily and regularly in the headlines. A list of recent data breaches involving lost or stolen laptops, where the data was *not* encrypted, is summarized in Table 1.

**Table 1: Recent Data Breaches Involving Lost or Stolen Laptops, Where Data was Not Encrypted**

| Disclosed | Organization | Records | Description |
|---|---|---|---|
| September 22, 2009 | Bernard Madoff Investors | 2,246 | Names, addresses, Social Security numbers and some account information was contained in a computer stolen from the car of an employee of AlixPartners LLP in Dallas. |
| September 2, 2009 | US Naval Hospital, Pensacola | 38,000 | The disappearance of a laptop computer compromised a database of 38,000 pharmacy service customers including names, Social Security numbers and dates of birth. |
| August 20, 2009 | Cal State University, Los Angeles | 600 | Two desktops and 12 laptop computers containing individual names, addresses and Social Security numbers were stolen from an office of the Minority Opportunities in Research program. |
| August 15, 2009 | Northern Kentucky University | 200 | An employee's laptop computer containing the Social Security numbers of at least 200 current and former students was stolen from a restricted area. |
| August 13, 2009 | National Guard Bureau | 131,000 | A laptop stolen from an Army contractor contained personal information on 131,000 soldiers, including names, Social Security numbers, incentive payment amounts and payment dates. |
| August 1, 2009 | Williams Cos. Inc. | 4,400 | A laptop containing names, birth dates, Social Security numbers, and compensation information for more than 4,400 current and former employees was stolen from a worker's vehicle. |
| July 29, 2009 | University of Colorado, Colorado Springs | 766 | A laptop containing class roster information – name, student ID number, e-mail address, graduating class year and grade information – for current and past students was taken from a professor's home. |
| July 17, 2009 | Francis Howell School District | 1,700 | A laptop computer stolen from the Human Resources department compromised the names and Social Security numbers of 1,700 school district employees. |
| June 30, 2009 | Sutter Health | 6,000 | A computer repair shop reported their possession of a laptop computer containing the names and Social Security numbers of 6,000 Sutter Health workers. |
| June 12, 2009 | Oregon Health & Science University | 1,000 | A physician's laptop containing patient names, treatment dates, short medical treatment summaries and medical record numbers was stolen from a car parked at the doctor's home. |
| May 13, 2009 | United Food & Commercial Workers Union | 19,000 | A union employee's laptop was stolen, exposing personal information including birth dates and Social Security numbers for 19,000 members of Local 555. |

Source: Privacy Rights Clearinghouse Chronology of Data Breaches, September 2009

## *Still More Regulatory Compliance*

In spite of the steady drip of data breach disclosures and an inherent desire to keep themselves out of similar headlines, *many companies still have not taken action* with respect to using file / folder encryption or full-disk encryption to safeguard the sensitive information of their shareholders, employees and customers. Predictably, this vacuum has led to additional government regulation, such as **201 CMR 17.00: Standards for the Protection of Personal Information of Residents of the Commonwealth of Massachusetts**. This law establishes minimum standards to be met in connection with the safeguarding of personal information contained in both paper and electronic records:

- *Every person that owns, licenses, stores or maintains personal information about a resident of the Commonwealth of Massachusetts and electronically stores or transmits such information shall include in its written, comprehensive information security program the establishment and maintenance of a security system covering its computers, including any wireless system, that, at a minimum, shall have … encryption of all personal information stored on laptops or other portable devices.*

Although awareness of 201 CMR 17.00 among affected companies is currently mixed, every entity that owns, licenses, stores or maintains personal information about a resident of the Commonwealth of Massachusetts must be in full compliance on or before *January 1, 2010*. This date has already been amended from the original deadline of January 1, 2009, to give affected companies more time to comply.

## *Industry Efforts to Improve Interoperability*

In addition to the heated public evidence of risk and the cold impetus of regulatory compliance, solution providers have stepped up their previously lukewarm investments designed to improve interoperability – and in turn, the practicality – of more widespread rollouts of endpoint encryption. Two important examples of such industry initiatives in 2009 are worthy of note:

- **Trusted Computing Group Storage Security Subsystem Class (OPAL) Specification** – The "Opal" specification provides a secure pre-boot authentication capability; facilities for the protection of user data from compromise due to loss, theft, repurposing or end of life of the drive; and administrative capabilities for user enrollment and media management. A half-dozen leading hard drive manufacturers and their software partners have announced support for hardware-based full-disk encryption products based on the Opal standard, several of which are already available in the market.
- **OASIS Key Management Interoperability Protocol (KMIP)** – By defining a protocol that can be used to request and deliver encryption keys between any key management system and any encryption system, KMIP is designed to help enterprises deploy a common enterprise key management infrastructure to manage

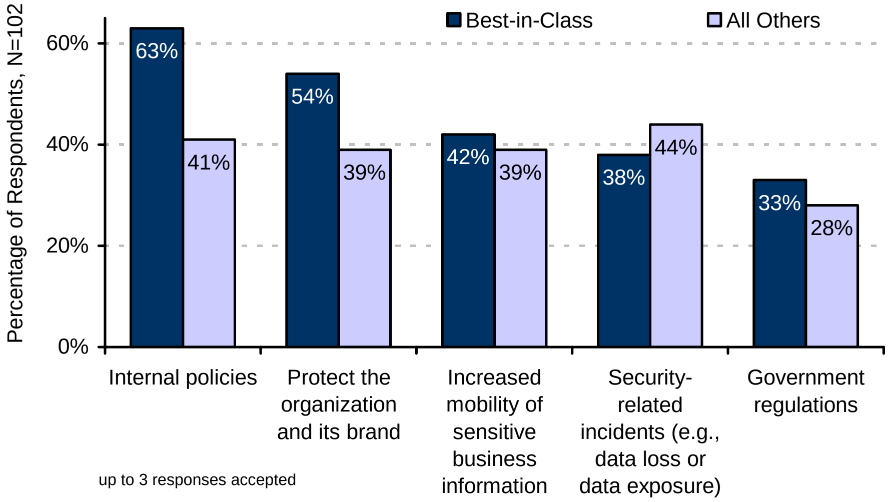
encryption keys (including symmetric keys, asymmetric key pairs, certificates and other security objects) for all encryption systems in the enterprise. Leading encryption and key management solution providers are actively collaborating on the KMIP standard.

## Top Drivers and Inhibitors for Endpoint Encryption

In Aberdeen's current study, **managing risks** associated with *protecting the organization and its brand*, specifically with respect to the *increased mobility of sensitive business information* are top drivers for current investment in endpoint encryption (Figure 2). Given enough time and repetition, headlines of lost or stolen laptops and tens of thousands of compromised records eventually do have an impact on IT Security budgets. Actual incidents of data loss or data exposure also act as drivers of current investments; Aberdeen's findings in this regard are summarized in Table 4.

Sustaining **compliance** is also a leading driver for current investments, although compliance with *internal policies* takes precedence over compliance with *government regulations*, *industry regulations*, and *industry standards and best practices*. In reality, internal policies are the integration and summing up of the matrix of compliance requirements such as Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry Data Security Standard (PCI DSS), Massachusetts 201CMR 17.00 and many others, as well as the integration and summing up of management's appetite for risk.

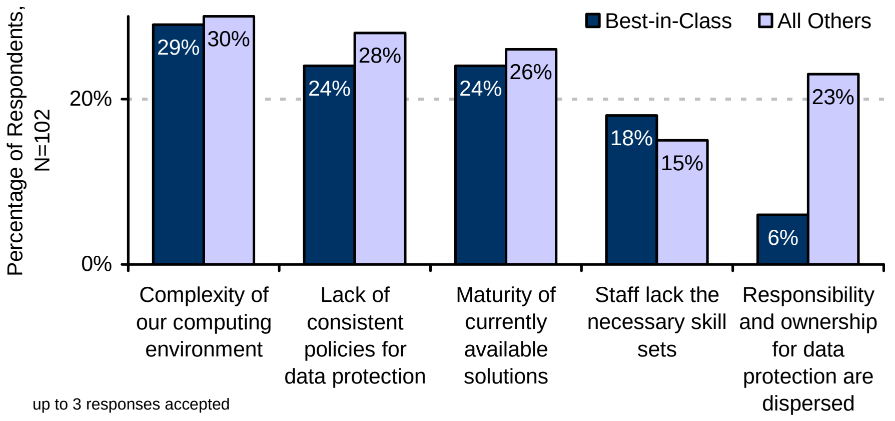
**Figure 2: Pressures Driving Investment in Endpoint Encryption**



Source: Aberdeen Group, September 2009

For respondents in the current study, the greatest **inhibitors** to current investments in endpoint encryption are the *complexity of their current computing environments*, and the *lack of consistent policies* for protecting data in use on endpoint systems (Figure 3). Best-in-Class organizations are notably different from all others in the study, being four-times less likely to have responsibility and ownership for data protection dispersed throughout the organization. Time and again Aberdeen's research confirms that holding someone accountable is consistently correlated with the companies that achieve top results.

**Figure 3: Inhibitors Preventing Investment in Endpoint Encryption**



Source: Aberdeen Group, September 2009

"Legacy hardware that cannot meet the minimum requirements for the software encryption solution is currently a roadblock. We cannot absorb a rip-and-replace strategy for this many existing systems."

~ IT Director,
>$5 billion Consumer
Electronics Company

Aberdeen's IT Security research agenda has covered aspects of this topic extensively over the last several quarters. In *Managing Encryption: The Keys to Your Success* (October 2008), best practices in key management and the encryption key lifecycle were profiled. In *Endpoint Security, Endpoint Management: The Cost-Cutter's Case for Convergence* (March 2009), the technologies and capabilities driving top performance in managing and protecting endpoints at the *platform*, *network*, *application* and *data* levels were described. In *Securing Unstructured Data: How Best-in-Class Companies Manage to Serve and Protect* (May 2009), four distinct strategies for safeguarding sensitive data were described and analyzed in terms of their correlation with Best-in-Class results. The current study focuses specifically on best practices in endpoint encryption, and is also intended to provide insights into how the companies that are achieving top performance are addressing the "space pen versus pencil" or "precise payloads versus more megatons" decision when it comes to implementing file / folder or full-disk encryption.

## Maturity Class Framework: Defining the Best-in-Class

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

- Number of security incidents (e.g., data loss or data exposure)
- Number of non-compliance incidents (e.g., audit deficiencies) related to endpoint encryption

- Amount of human error (e.g., policy violations) related to endpoint encryption

In addition, Aberdeen used the number of intentional data loss or data exposure incidents from internal sources (e.g., non-malicious violations of policy by well-intentioned end-users trying to carry out their everyday tasks) experienced over the last 12 months. The first two criteria were selected as measures of an organization's performance in improving security and compliance related to endpoint encryption, while the final two were selected as indicators of operational control. 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 7 in Appendix A.)

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

| Definition of Maturity Class | Mean Class Performance (last 12 months) |
|---|---|
| **Best-in-Class: Top 20%** of aggregate performance scorers | ▪ **6.7% reduction** in the total number of actual data loss or data exposure incidents<br>▪ **2.8% reduction** in the number of non-compliance incidents (e.g., audit deficiencies) related to endpoint encryption<br>▪ **2.1% reduction** in human error related to endpoint encryption (e.g., policy violations)<br>▪ **0** incidents of data loss or data exposure from internal sources (intentional, e.g., as a result of well-intentioned, non-malicious policy violations) |
| **Industry Average: Middle 50%** of aggregate performance scorers | ▪ **0.8% increase** in the total number of actual data loss or data exposure incidents<br>▪ **2.6% reduction** in the number of non-compliance incidents (e.g., audit deficiencies)<br>▪ **0.6% increase** in human error related to endpoint encryption (e.g., policy violations)<br>▪ **5** incidents of data loss or data exposure from internal sources (intentional) |
| **Laggard: Bottom 30%** of aggregate performance scorers | ▪ **2.1% increase** in the total number of actual data loss or data exposure incidents<br>▪ **8.9% increase** in the number of non-compliance incidents (e.g., audit deficiencies)<br>▪ **8.9% reduction** in human error related to endpoint encryption (e.g., policy violations)<br>▪ **6** incidents of data loss or data exposure from internal sources (intentional) |

Source: Aberdeen Group, September 2009

## The Best-in-Class PACE Model

Safeguarding critical data in use at the endpoints using encryption 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 6 in Appendix A). The characteristics exhibited by Best-in-Class organizations in this study are summarized in Table 3.

**Table 3: Best-in-Class PACE Framework for Endpoint Encryption**

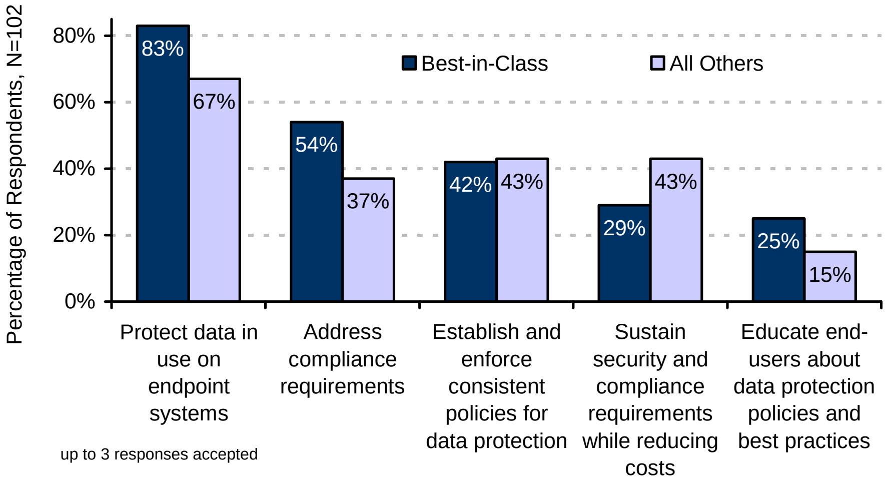
| Pressures | Actions | Capabilities | Enablers (% of Best-in-Class Adoption) |
|---|---|---|---|
| ▪ Internal policies<br>▪ Protect the organization and its brand | ▪ Protect data in use on endpoint systems<br>▪ Achieve compliance with regulations, policies, standards and / or best practices that impact data protection<br>▪ Establish and enforce consistent policies and procedures for data protection | ▪ Discovery of all information assets<br>▪ Information classified by requirements for confidentiality, integrity and availability<br>▪ Systematic implementation / rollout processes for encryption solutions<br>▪ Responsible executive or team with primary ownership for endpoint encryption initiatives<br>▪ Formal documentation, awareness and training programs for end-users<br>▪ Automatic enforcement of data protection policies (transparent to end-users)<br>▪ Consistent, unified view of information and events related to endpoint encryption<br>▪ Centralized management of configurations and policies<br>▪ Centralized management of the encryption key lifecycle<br>▪ Effective measurement of the number of data loss or data exposure incidents, including source (channels, users) | ▪ Full-Disk Encryption (91%)<br>▪ File / Folder encryption (77%)<br>▪ USB drive encryption (50%)<br>▪ Removable media encryption, e.g., DVD, CD, SD (23%)<br>▪ Enterprise Rights Management (32%)<br>▪ Enterprise Key Management (15%)<br>▪ Anti-theft devices, i.e., physical security (53%) |

Source: Aberdeen Group, September 2009

## Best-in-Class Strategies and Results

It came as no surprise that when asked about strategic actions that are driving their current investments in endpoint encryption, Best-in-Class companies identified **protect data in use on endpoint systems** and **address compliance requirements** as being of top importance (Figure 4). **Establishing consistent policies**, and **educating end-users** about those policies, are also characteristic strategies of the top performers. **Reducing the total associated cost** of security and compliance is also one of the top strategic drivers, consistent with the Best-in-Class pattern of first ensuring that their IT infrastructures are *secure*, then *compliant*, and then *optimized* for efficiency and effectiveness.

**Figure 4: Strategies Driving Investment in Endpoint Encryption**



Source: Aberdeen Group, September 2009

## *Why Top Performance Matters: Lower Risk, Lower Cost*

Aberdeen's research shows that Best-in-Class organizations have reduced the costs related to endpoint encryption in several ways, including year-over-year reductions in:

- The number of data loss or data exposure incidents, and the average time and cost to address them
- The number of audit deficiencies, and the average time and cost to address them
- The amount of human error (e.g., policy violations)
- The number of help desk calls
- The number of full-time equivalent administrators

The average number of data loss or data exposure incidents respondents experienced in the last 12 months is summarized, by type of incident, in Table 4. In general, the research confirms that external (*malicious*) breaches are outweighed by internal breaches caused by simple human error (*inadvertent*) and by well-meaning employees violating policies while trying to carry out their jobs (*intentional*). Overall, the top-performing organizations experienced six-times fewer data loss or data exposure incidents as compared to the bottom performers in the study.

**Table 4: Average Number of Data Loss or Data Exposure Incidents Experienced in the Last 12 Months, by Type**

| Type of Data Loss or Data Exposure Incident | Best-in-Class | Industry Average | Laggard |
|---|---|---|---|
| Internal – inadvertent (end-user error) | 2 | 7 | 8 |
| Internal – intentional (non-malicious violation of policies) | 0 | 5 | 6 |
| External (malicious) | 1 | 5 | 5 |
| **Total** | **3** | **17** | **19** |

Source: Aberdeen Group, September 2009

Findings from *The 2009 Aberdeen Report* showed that the average total financial impact for each data loss or data exposure incident is approximately US$640,000. Based on this estimate, the advantage of achieving top performance – i.e., the relative performance of the Best-in-Class companies in comparison to that of Laggards – translates to 16 fewer incidents per year, times $640,000 per incident, or about $10 million per year in costs avoided.

On an operational level, respondents were asked to estimate the annual total cost of ownership for their endpoint encryption initiatives. When normalized in terms of average total cost per end-user per year, the top performers spent $53 while lagging performers spent $86, a 40% advantage for Best-in-Class performance. Depending on the total number of endpoints in your organization, the cumulative effect of $33 savings per endpoint per year can make a compelling business case for pursuit of best practices in endpoint encryption. In the next chapter, we will see what the top performers are doing to achieve these gains.

**Aberdeen Insights – Strategy**

In the strategic decision enterprises make between the precision of file / folder encryption (encrypting only specific files or folders based on content and pre-existing policies) and the brute force of full-disk encryption (encrypting everything on the endpoint), Aberdeen's research shows that the general trend is towards the simplicity of full-disk encryption. This trend is observable over the course of several benchmark studies in data protection which Aberdeen has conducted over the past two years, and is expected to continue.

Both approaches are widely deployed and the shift has been gradual, not sudden. In the current study, Best-in-Class organizations are about equally as likely to rely on end-user based enforcement of data protection policies (unaided by solutions) as they are to enforce data protection policies automatically (transparent to end-users). In comparison to Laggards, however, they are three-times more likely to automate enforcement transparent to end-users.

*continued*

"We are just beginning to evaluate full-disk encryption solutions. It needs to be plug-and-play with our existing endpoints, including both Windows and Mac. It needs to be fast and easy to roll out, so we can meet compliance-driven deadlines. It also needs good management and reporting capabilities, to reduce management costs and address our auditing requirements."

~ IT Manager,
Massachusetts Law Firm

### Aberdeen Insights – Strategy

In addition to a shift towards not relying on the correct behavior of individual end-users, Aberdeen's research indicates a shift towards not investing time and effort into developing fine-grained policies to address a complex and constantly changing compliance landscape. Best-in-Class organizations are consistently more likely than their Industry Average and Laggard counterparts to map security risks and corresponding controls to their particular matrix of compliance requirements, not the other way around. As a simple example, "if resident of Massachusetts, then encrypt all personal information stored on laptops" becomes "encrypt all information stored on laptops."

Chasing compliance requirements one at a time can lead to both overlaps (resulting in higher cost) and gaps (resulting in increased security incidents, and increased audit deficiencies) in controls. The "checkbox" approach to compliance consumes undue attention and resources, and makes it harder to succeed at the game of "do more with less." The Best-in-Class approach to IT security is to be secure first, then compliant; they are getting to a risk-based – as opposed to a regulation-based – view of protecting the business.

# Chapter Two: Benchmarking Requirements for Success

The selection of file / folder or full-disk encryption – along with the policy, planning, process, and organizational elements of implementation – are critical success factors in the ability to realize the business benefits of enhanced security, sustained compliance, and more cost-effective ongoing operations.

### Case Study – Fabless Semiconductor Company, California

A California-based fabless semiconductor company focuses on Intellectual Property (IP) for special-purpose processors which are designed to enable real-time image processing and analytical capabilities for security, defense, machine vision, robotics, guidance systems, manufacturing monitoring and control, and other markets. The company designs, verifies, simulates and produces these processors using the latest available technologies. Protection of the company's IP is so paramount that a formal non-disclosure agreement is required before prospective customers are provided with any detailed description or documentation.

Most of the company's data is stored on centralized, well-protected servers. All network communication is encrypted using IP-Sec VPNs with random number generated keys. All laptops in the environment use full-disk encryption, though stationary desktop computers and workstations currently do not. The use of removable media is closely monitored and minimized. The company also invests in user education and training with respect to data security, including regular reminders to store and protect important intellectual property on the corporate servers.

"With our standard laptop configurations we are now specifying hardware-based full-disk encryption, there's no incremental cost and very little added complexity," noted the company's CTO and Vice President of Engineering. "Between this and support from third parties there are now several viable FDE options. It's also easy enough that we haven't experienced the need to work through an integrator."

To date, results of the full-disk encryption implementation match the company's expectations. If anything, the company has felt the need to give additional attention to its processes for data backup and recovery: "FDE does exactly what it says. Trying to recover information from an FDE-protected disk after the laptop is lost or stolen is impossible. We now take extra steps to ensure that backups are made regularly, and that the backups contain the data the users think they contain."

## Competitive Assessment

Aberdeen analyzed the aggregated metrics of surveyed companies to determine whether their performance in endpoint encryption ranked as

**Fast Facts**

Average annual total cost of ownership per end-user (US$ per end-user per year) for endpoint encryption, by Maturity Class

√ Best-in-Class: $53

√ Industry Average: $59

√ Laggards: $86

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 ability of the organization to measure results to improve the business). These characteristics, identified in Table 5, serve as a guideline for best practices, and correlate directly with Best-in-Class performance across the associated metrics.

**Table 5: Competitive Framework for Endpoint Encryption**

| | Best-in-Class | Average | Laggards |
|---|---|---|---|
| **Process** | Information classified by requirements for confidentiality, integrity and availability | | |
| | 56% | 51% | 50% |
| | Systematic implementation / rollout processes for encryption solutions | | |
| | 44% | 36% | 12% |
| **Organization** | Responsible executive or team with primary ownership for endpoint encryption initiatives | | |
| | 62% | 53% | 41% |
| | Formal documentation, awareness and training programs for end-users | | |
| | 50% | 44% | 33% |
| **Knowledge Management** | Discovery of all information assets | | |
| | 41% | 34% | 24% |
| | Consistent, unified view of information and events related to endpoint encryption | | |
| | 35% | 23% | 0% |
| **Technology / Automation** | End-user based enforcement of data protection policies (unaided by solutions) | | |
| | 48% | 42% | 38% |
| | Automatic enforcement of data protection policies (transparent to end-users) | | |
| | 41% | 33% | 13% |
| | Centralized management of configurations and policies | | |
| | 58% | 43% | 41% |
| | Centralized management of the encryption key lifecycle | | |
| | 41% | 32% | 31% |
| | For current use of endpoint encryption and related technologies, see **Figure 5** and **Figure 6** | | |

| | Best-in-Class | Average | Laggards |
|---|---|---|---|
| **Performance Management** | Track number of data loss or exposure incidents | | |
| | 65% | 40% | 29% |
| | Track source (channels) of data loss or exposure incidents | | |
| | 60% | 29% | 19% |
| | Track source (users) of data loss or exposure incidents | | |
| | 56% | 34% | 19% |

Source: Aberdeen Group, September 2009

## 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 endpoint encryption beyond that of their Industry Average and Laggard counterparts.

"Based on a problem we experienced, companies should pay close attention to the support infrastructure provided by their vendors to assist in recovering from software defects and/or inherent design problems. When a vendor accepts money to protect your critical data, they should have the tools and the people in place to assist you when their errors deny access to that data."

~ CEO, < $50 million High-Tech Company

### *Process*

There is relatively little difference between the three maturity classes in terms of classifying information based on requirements for confidentiality, integrity and availability – but the approach of encrypting everything at the endpoint makes such classification far less important. Investments in systematic implementation and rollout processes for encryption solutions is a much greater differentiator; Best-in-Class organizations are four-times more likely than Laggards to indicate these as a current capability. Top performance in this area is a significant contributor to the savings of $33 per endpoint per year realized by the Best-in-Class (i.e., total cost of ownership for endpoint encryption of $53 per endpoint per year for Best-in-Class organizations, compared to $86 per endpoint per year for Laggards).

### *Organization*

In study after study, Aberdeen's research confirms that having an executive or team with primary ownership for an important cross-enterprise initiative is strongly correlated with the companies that achieve top results. This study is no exception to the venerable "one throat to choke" principle. Similarly, the current findings fit the typical pattern that top performers are more likely than their counterparts to invest in documentation, awareness and training for end-users. Note that the use of full-disk encryption or the automatic and transparent enforcement of policies does not eliminate the need for end-user awareness and training. On the contrary, end-users still need to be made aware of policies and expectations for behavior with respect to sensitive data, and held accountable. Moreover, end-user expectations should be set regarding topics such as authenticating to access encrypted data, performance of encrypted endpoints, IT monitoring and reporting practices, and so on.

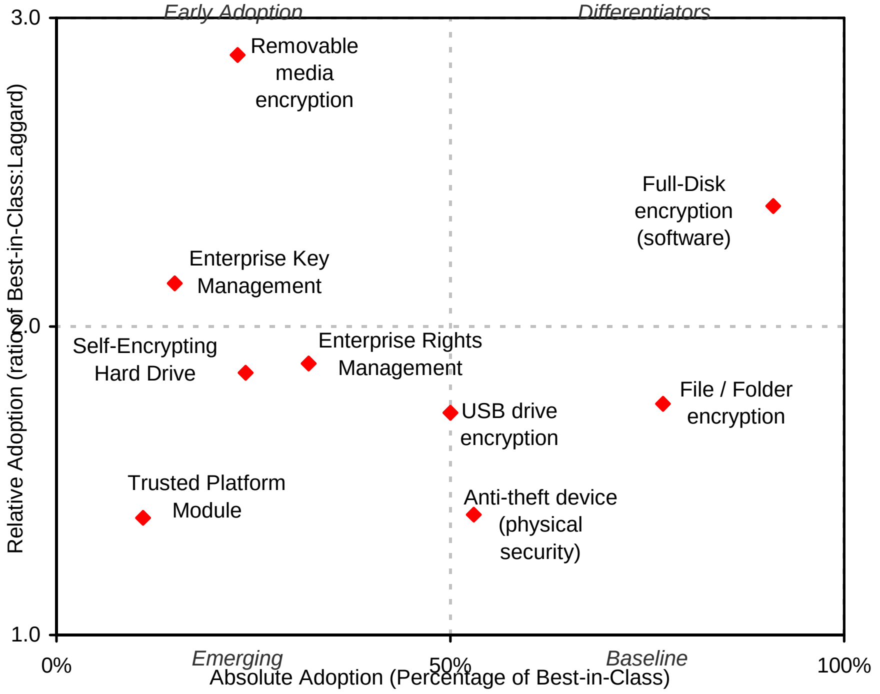
## Knowledge Management

Just one-third (35%) of the Best-in-Class organizations in the study indicated that they have a consistent, unified view of information and events related to endpoint encryption, compared to none of the Laggards. Companies still need to be able to demonstrate to auditors that policies for safeguarding sensitive information are being enforced, or to provide assurance that sensitive data on a lost or stolen laptop was in fact encrypted. The latter is particularly important, for example, to qualify for the safe harbor exemptions to data breach disclosure laws such as California Senate Bill 1386 and its many equivalents in other US states … and thereby keep the company off the growing list of disclosures as shown in Table 1.

## Technology / Automation

Best-in-Class organizations in this study are about equally as likely to rely on end-user based enforcement of data protection policies (unaided by solutions) as they are to enforce data protection policies automatically (transparent to end-users). This is consistent with the fact that both file / folder encryption and full-disk encryption currently enjoy widespread deployment. In comparison to Laggards, however, Best-in-Class companies are three-times more likely to enforce encryption automatically and transparently to the end-users, greatly reducing the probability of internal breaches caused by simple human error (*inadvertent*) and by well-meaning employees violating policies while trying to carry out their jobs (*intentional*).

**Figure 5: Best-in-Class Absolute, Relative Adoption of Technology**



Source: Aberdeen Group, September 2009

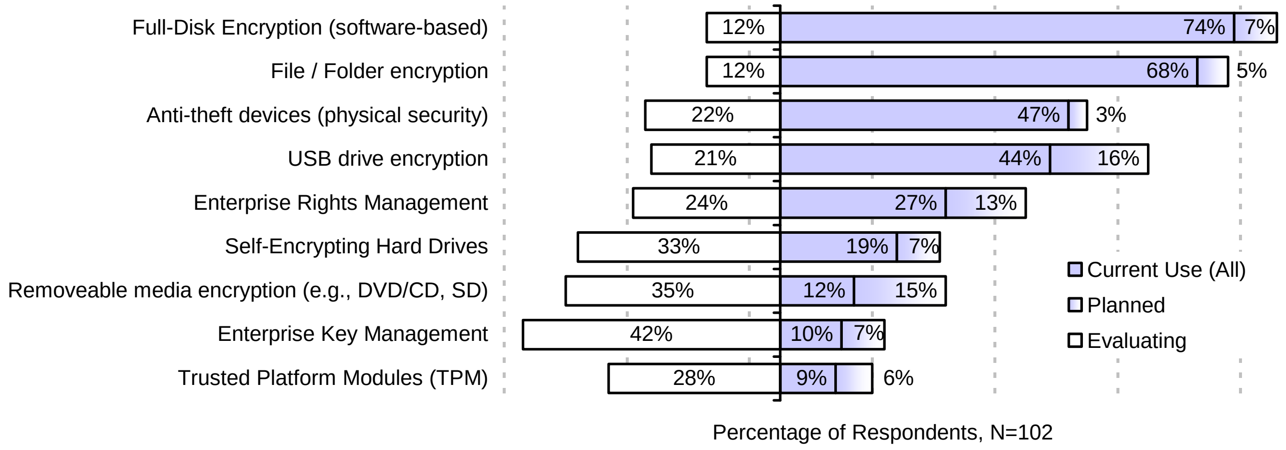
Current use of various enabling technologies by the Best-in-Class organizations in the current study is shown in Figure 5, plotted against the relative use by the Best-in-Class as compared to that of Laggards. *File / folder encryption* is found in the lower right-hand quadrant, indicating current use by a high percentage of both Best-in-Class and Laggard organizations. This reflects the widespread historical use of file / folder encryption as an option to protect sensitive data in use at the endpoints. Another **baseline** technology is *anti-theft devices*, i.e., physical security solutions for endpoint systems. This is almost another "space pen versus lead pencil" story within the endpoint encryption story, in the sense that a low-tech anti-theft solution may have been highly effective at preventing several of the stolen laptops among the public data breach disclosures described in Table 1.

*USB drive encryption* is another solution that appears to be moving rapidly towards the baseline technologies quadrant, while *encryption of removable media* (DVDs, CDs, SD) is currently in the **early adoption** phase among Best-in-Class companies. Aberdeen plans a follow-on benchmark study focused specifically on security for mobile endpoint devices – including USB drives, smart phones, and removable media – in the near future.

*Enterprise key management* is also in the early adoption quadrant of Figure 5. Aberdeen's research on *The Encryption Key Lifecycle* (November 2008) showed that to support the broader deployment of encryption – and to reduce the cost of managing encryption and the encryption key lifecycle – organizations with top performance have looked towards increased automation and centralized, heterogeneous approaches to key lifecycle management. In doing so, they are delivering the tangible benefits of improved security, sustained compliance, and lower operational costs.

*Full-disk encryption* appears in the upper-right quadrant of Figure 5, which indicates high Best-in-Class adoption in absolute terms, as well as high adoption by the Best-in-Class relative to Laggards. This makes full-disk encryption a **differentiator** of top performance in the current study.

**Figure 6: Technology Adoption Trends: Current Use, Planned Within 12 Months, Evaluating (all)**



Source: Aberdeen Group, September 2009

A different take on the findings for enabling technologies is provided in Figure 6. Current use of various technologies for all respondents is shown along with planned use in the next 12 months and current evaluations. Planned use versus current use can be taken as a rough proxy for near-term market opportunity; for example, the findings in Figure 6 indicate very strong near-term growth for the *encryption of USB drives* and *removable media*. Current evaluations are a good indicator of the current level of market interest, which again shows very strong interest in encryption of USB drives and removable media, and also for the new generation of *self-encrypting hard drives*. As the deployments of encryption increases, so does the need for *enterprise key management*, which supports the extremely high level of current evaluations shown in Figure 6.

## *Performance Management*

Regardless of the selected approach to endpoint encryption, the leading performers are two-times to three-times more likely than lagging performers to track the number of data loss or data exposure incidents, and the source of these incidents both by channel and by end-user. A better understanding of the patterns of these breaches can help to identify the need for complementary controls (such as content monitoring / filtering) or the need to change end-user behavior. It could also help to identify the need to change policies: "Nothing is worse than great enforcement of a bad policy," as the CTO of a scientific research lab put it. Or as the managing director of a small services firm colorfully commented, "Let's put a stop to stupid."

### Aberdeen Insights – Technology

Over the course of several benchmarks in the last two years, Aberdeen has found that the use of file / folder encryption is gradually giving way to the more widespread use of full-disk encryption. Forward-looking providers of full-disk encryption solutions have invested in the **platform coverage** (including Windows, Mac and Linux), **technical certifications** (such as FIPS 140), **key lifecycle management** capabilities (including interoperability initiatives such as KMIP), and flexible options for **pre-boot authentication** (including both passwords and stronger methods) that are required to make full-disk encryption an increasingly viable and acceptable choice, along with the recovery, management, auditing and reporting capabilities that are necessary for large-scale enterprise deployment.

The debate between the merits of *hardware-based* full-disk encryption and *software-based* full-disk encryption are somewhat academic, as the leading solution providers will inevitably adapt their solutions to support flexibility and choice in this regard. In the long term, it seems likely that hardware-based cryptography will become the foundation for most endpoint encryption, based on inherent advantages in security, performance, and out-of-the-box support. Buyers should look for solutions that take an ecumenical, mix-and-match approach in this regard.

# Chapter Three: Recommended Actions

Whether a company is trying to move its performance in endpoint encryption from Laggard to Industry Average, or Industry Average to Best-in-Class, the following actions will help drive the necessary improvements.

## Laggard Steps to Success

- **Do something.** Whether driven by the ample evidence of the risk of data loss or data exposure or by the complex and changing landscape of compliance requirements, how much more compelling does the case for protecting data in use at the endpoints need to be before Laggards will take action? Regardless of which approach to endpoint encryption is taken, all companies should be doing *something* to mitigate this risk.
- **Select an approach.** Both file / folder encryption and full-disk encryption are widely deployed, though Aberdeen's research shows that between the precision of encrypting only specific files or folders based on content and pre-existing policies, versus the brute force of encrypting everything on the endpoint, the general trend is towards the simplicity of full-disk encryption.

## Industry Average Steps to Success

- **Integrate encryption with existing processes.** New or replacement endpoint systems should be pre-configured with the selected encryption option. Password recovery and emergency access facilities should be integrated with existing helpdesk processes. Existing backup and recovery, patch management, and other automated or unattended processes should be adapted to accommodate encrypted endpoints. Training for end-users should communicate and set expectations – in plain language – regarding authentication, performance, monitoring, and so on. The extent to which endpoint encryption can be made systematic and integral to these types of processes will be the biggest gating factor to success, particularly on large-scale rollouts.
- **Enforce automatically.** Aberdeen's research shows a strong trend away from reliance on individual end-users to make the right decisions about which files and folders on their endpoint systems should be encrypted. Full-disk encryption (and some file / folder encryption solutions) enforces encryption automatically and transparently to the end-users, greatly reducing the probability of inadvertent or well-meaning but intentional violations of policy.

Fast Facts

Rating of the level of automation of the key management lifecycle, on a scale of 1=lowest to 5=highest

√ Best-in-Class: 2.73

√ All Others: 1.97

Current capability for centralized destruction of encrypted data ("digital shredding")

√ Best-in-Class: 19%

√ Industry Average: 11%

√ Laggards: 7%

## Best-in-Class Steps to Success

- **Centralize management.** Centralized management of encryption configuration and policies is correlated with top performance, as is centralized management of the encryption key lifecycle. Companies should expand their use of encryption with a strategic approach to the key lifecycle in mind, from cradle (initial generation, distribution, and integration with encryption-enabled applications), to productive lifetime, to grave (eventual revocation and destruction). Centralized, audited processes to recover access to encrypted data – or to cryptographically "shred" encrypted data on lost, stolen or repurposed endpoints – are examples of the tangible control that Best-in-Class companies exercise over their endpoint encryption deployments.

### Aberdeen Insights – Summary

Ample public evidence of the risk of loss or exposure of sensitive data, in combination with a complex and changing landscape of compliance requirements, make a compelling case for protecting data in use at the endpoints using encryption. In addition, solution providers are increasing their investments to simplify deployment and improve interoperability. The case for endpoint encryption that many IT Security professionals have argued for many years has become easier, although the practical matters of priority, total cost, and effective deployment and management must still be addressed as always.

Aberdeen's research shows a general trend towards the simplicity of encrypting everything on the endpoint using full-disk encryption, as compared to the precision of encrypting only specific files or folders based on content and pre-existing policies using file / folder encryption. Both approaches are widely deployed, but the benchmark results over the last two years make it clear that full-disk encryption is on the rise.

While just 10% of all respondents in the current study indicated that they are currently using solutions for centralized, heterogeneous key management (i.e., not a native feature of a point encryption solution), an eye-opening 42% indicated that they are currently evaluating key management solutions and another 7% indicated plans to deploy within the next year. As the use of encryption continues to proliferate throughout the enterprise, strategic investments in a scalable and cost-efficient approach to managing the encryption key lifecycle remain the keys to success for Best-in-Class deployments.

# Appendix A:
# Research Methodology

In September 2009, Aberdeen examined the experiences and intentions of more than 100 organizations from a diverse set of industries. Aberdeen supplemented this online survey effort with telephone interviews with select survey respondents, gathering additional information on endpoint encryption 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 (18%); Vice President / General Manager (9%); Director (23%); Manager (16%); Staff / Consultant (28%); and other (6%). The largest segment by functional responsibility was IT, representing 55% of the total sample.
- **Industry:** The research sample included respondents from a wide range of industries. The largest segments included financial services (8%), telecommunications (8%) and government / aerospace / defense (18%).
- **Geography:** A majority of respondents (62%) were from the Americas. Remaining respondents were from the Asia-Pacific region (8%) and Europe / Middle East / Africa (30%).
- **Company size:** Twenty-eight percent (28%) of respondents were from large enterprises (annual revenues above US $1 billion); 29% were from midsize enterprises (annual revenues between $50 million and $1 billion); and 43% of respondents 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 technologies are deployed as part of their IT operations, and the financial impact of these technologies

√ The efficiency and effectiveness of existing implementations

√ Benefits that have been derived with respect to enhanced security, sustained compliance, and reduced operational costs

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

### Table 6: 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, September 2009

### Table 7: 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, September 2009

### Table 8: 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, September 2009

# Appendix B:
# Related Aberdeen Research

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

- *Enterprise Rights Management: Persistence Pays Off*; August 2009
- *File Transfer is Not What it Used to Be: It's Secure, Reliable and Well-Managed*; July 2009
- *Microsoft SharePoint: The Comedy (and Tragedy) of the Commons*; 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
- *PGP Expands Full-Disk Encryption Market by Adding Managed Service Providers*; April 2009
- *Endpoint Security, Endpoint Management: The Cost-Cutter's Case for Convergence*; March 2009
- *Protecting the Database*; November 2008
- *Managing Encryption: The Keys to Your Success*; October 2008
- *The Encryption Key Lifecycle*; November 2008
- *Making Progress in PCI Compliance: Protecting Data at Rest, in Motion, and in Use*; September 2008
- *PCI DSS and Protecting Cardholder Data: Year-over-Year Progress in Achieving, and Sustaining, Compliance*; June 2008
- *Data Loss Prevention: Little Leaks Sink the Ship*; June 2008

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

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

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

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