

# **Thwarting Data Loss**

*Best in Class Strategies for Protecting Sensitive Data*

May 2007

## Executive Summary

Ongoing reports of data breaches bring home the reality that organizations are seriously vulnerable to assaults on their digital assets. Legislation forcing companies to disclose these incidents is elevating what has been “a dirty little secret” into primetime news. This Aberdeen report looks at how Best in Class companies protect their sensitive data.

### Best in Class Performance

Aberdeen used four key performance criteria to distinguish Best in Class:

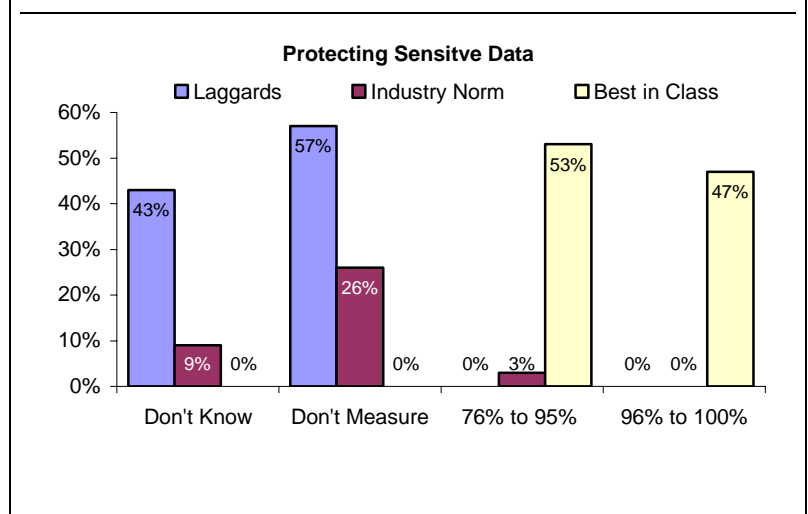
- Percentage of sensitive data protected from insider threat
- Percentage of sensitive data protected from external threat
- Decrease in the number of data breaches compared to one year ago
- Increase in percentage of sensitive data protected from insider threat or external threat.

### Competitive Maturity Assessment

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

- They are four times more likely to use real-time notification of inappropriate data use than industry laggards
- They train employees in appropriate data use
- They monitor and audit data use
- They view regulatory compliance as a top driver

Figure 1: Attending to Data Use



### Required Actions

In addition to the specific recommendations in chapter 3 of this report, to achieve Best in Class performance, organizations must:

- Identify and classify sensitive data throughout systems – in email, spreadsheets, and wherever it resides
- Create a data use policy and hold users responsible with clear consequences for inappropriate use
- Enforce regulatory compliance

[Send to a Friend](#) 

## Table of Contents

Executive Summary.....	2
Best in Class Performance.....	2
Competitive Maturity Assessment.....	2
Required Actions .....	2
Chapter One: Benchmarking the Best in Class.....	4
Maturity Class Framework .....	5
Best in Class PACE Model.....	5
Chapter Two: Benchmarking Requirements for Success .....	8
Competitive Assessment.....	8
Organizational Capabilities and Technology Enablers .....	9
Chapter Three: Required Actions .....	12
Laggard Steps to Success.....	12
Industry Norm Steps to Success .....	12
Best in Class Steps to Success .....	12
Appendix A: Research Methodology.....	14
Appendix B: Related Aberdeen Research.....	17

## Figures

Figure 1: Attending to Data Use.....	2
Figure 2: Top Pressures driving Companies to focus on Protecting their Data .....	4
Figure 3: Capabilities deployed by Best in Class vs. Industry Norm.....	6
Figure 4: Technology Adoption in Laggards vs. Industry Norm .....	10

## Tables

Table 1: Companies With Top Performance Earn “Best in Class” Status: .....	5
Table 2: Best in Class PACE Framework .....	6
Table 3: Competitive Framework.....	9
Table 4: PACE Framework .....	15
Table 5: Maturity Framework.....	15
Table 6: Relationship between PACE and Competitive Framework.....	16

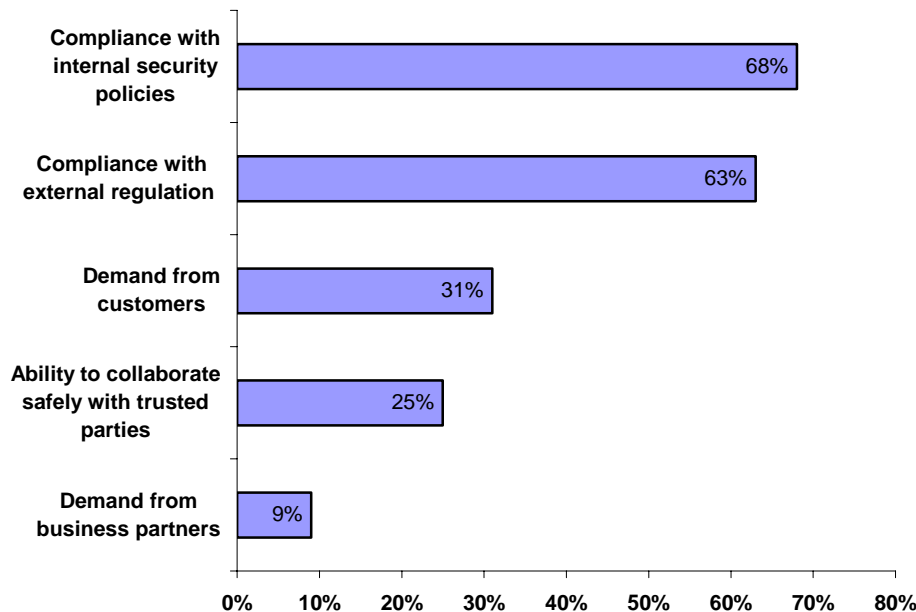
## Chapter One: Benchmarking the Best in Class

No company or organization of stature is exempt from the peril represented by a breach of its sensitive data.

Many companies are at risk simply as a result of doing business with the tools at hand without focusing on the vulnerabilities inherent in their use. For example, without careful consideration and definition of usage groups, organizations default to an open stance, allowing the easy access and sharing that seems to let everyone get their work done with the fewest obstacles. In an ideal world where everyone's intentions are honorable and no one ever makes mistakes, this might make sense. In the real world it is both foolhardy and irresponsible.

Aberdeen Group surveyed more than 150 organizations about their approach to protecting sensitive data. This report looks at how the Best in Class are contending with the challenge of protecting sensitive data.

**Figure 2: Top Pressures driving Companies to focus on Protecting their Data**



Source: Aberdeen Group, May 2007

### Fast Facts

- √ *Best in Class companies are **more than twice as likely** to have reduced the number of data loss / data leak incidents over the past 12 months as compared to the Industry norm..*
- √ *Best in Class companies are **10 times more likely** to have reduced their total financial loss associated with data loss incidents over the last 12 months compared with Laggard companies.*

### Major Bank

We were a lot safer when everything we needed to protect was in one location, and we could tightly control who could enter that one location. Today, we're trying to secure information and at the same time make it available everywhere to anyone who needs it.

**Security Consultant  
IT Management Staff**

## Maturity Class Framework

Aberdeen used five key performance criteria to distinguish Best in Class companies from Industry Average and Laggard organizations.

Table 1: Companies With Top Performance Earn “Best in Class” Status:

Definition of Maturity Class	Mean Class Performance
<p><b>Best in Class:</b> Top 20% of aggregate performance scorers</p>	<ul style="list-style-type: none"> <li>• <b>31%</b> protect at least 96% of their sensitive data from insider threats</li> <li>• <b>65%</b> protect at least 96% of their sensitive data from external threats</li> <li>• <b>66%</b> increased the percentage of sensitive data protected from insider threats in the last year</li> <li>• <b>77%</b> increased the percentage of sensitive data protected from external threats in the last year</li> <li>• <b>62%</b> reduced the number of data loss/leakage incidents last year over the year before</li> </ul>
<p><b>Industry Average:</b> Middle 50% of aggregate performance scorers</p>	<ul style="list-style-type: none"> <li>• <b>0%</b> protect at least 96% of their sensitive data from insider threats</li> <li>• <b>17%</b> protect at least 96% of their sensitive data from external threats</li> <li>• <b>53%</b> increased the percentage of sensitive data protected from insider threats in the last year</li> <li>• <b>64%</b> increased the percentage of sensitive data protected from external threats in the last year</li> <li>• <b>30%</b> reduced the number of data loss/leakage incidents last year over the year before</li> </ul>
<p><b>Laggard:</b> Bottom 30% of aggregate performance scorers</p>	<ul style="list-style-type: none"> <li>• <b>0%</b> protect at least 96% of their sensitive data from insider threats</li> <li>• <b>0%</b> protect at least 96% of their sensitive data from external threats</li> <li>• <b>5%</b> increased the percentage of sensitive data protected from insider threats in the last year</li> <li>• <b>5%</b> increased the percentage of sensitive data protected from external threats in the last year</li> <li>• <b>0%</b> reduced the number of data loss/leakage incidents last year over the year before</li> </ul>

Source: Aberdeen Group, May 2007

## Best in Class PACE Model

The Best in Class report that their top pressure (propelling them to protect their data) is compliance with external regulations and internal security policies. To address this pressure they take the actions, require the capabilities and use the enablers summarized in the PACE framework below.

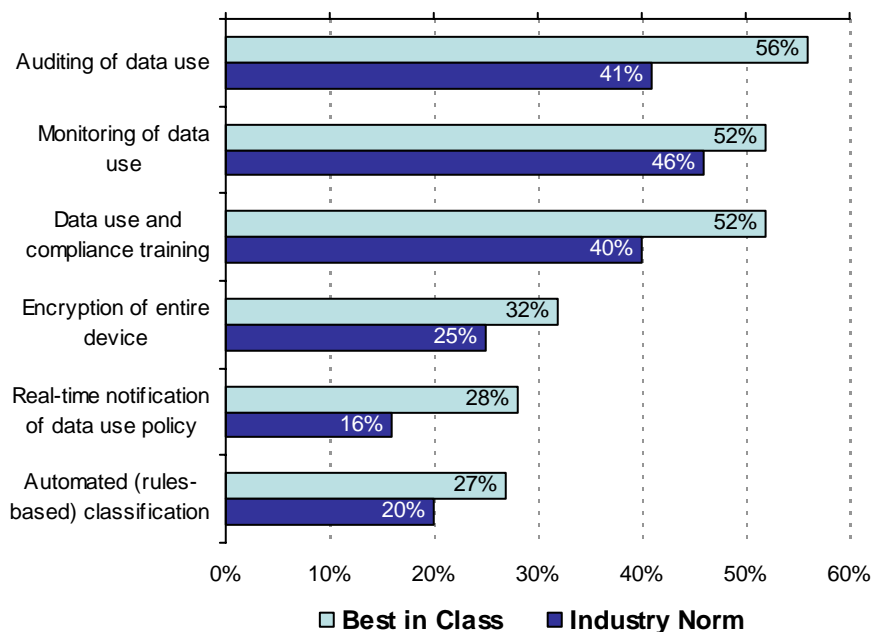
**Table 2: Best in Class PACE Framework**

Pressures	Actions	Capabilities	Enablers
Compliance with External Regulations and Internal Security Policies	Identify and protect sensitive data  Deploy end-to-end data protection  Attain regulatory compliance	Definition and Enforcement of Data Use Policy  Discovery of Sensitive Data  Training in data use and compliance requirements  Monitoring, auditing and reporting of data use  Encryption on the file, folder and device level	Data loss prevention solutions  Web filtering  Anti-phishing / pharming / spyware solutions  Encryption and key management solutions  Enterprise rights management solutions

Source: Aberdeen Group, May 2007

Best in Class companies are further along in their applying critical capabilities to the problem of data loss prevention.

**Figure 3: Capabilities deployed by Best in Class vs. Industry Norm**



Source: Aberdeen Group, May 2007

### Aberdeen Insights – Strategy

Although many companies surveyed cite compliance with external regulations as a driver in their pursuit of protecting sensitive data, Best in Class companies are more apt to name it a top priority and more apt to state the attainment of regulatory compliance as an explicit action they're pursuing. It appears that the need to prove compliance is helping companies identify and solve the issues associated with protecting their sensitive data. Without the external pressures to comply and the requirements forcing companies to disclose data breaches, companies are more apt to live with the status quo and gamble with the odds that they're safe or willing to live with the consequences of a breach.

Despite claims they've made efforts to secure more of their data over the past year, many companies report that the incidence of data loss has remained at the same level or gotten worse. Cyber crime is big business and we can anticipate that the number of attacks will continue to grow, and that the sophistication of the attacks will grow as well. Companies that ignore these threats put themselves at great risk.

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

## Chapter Two: Benchmarking Requirements for Success

The selection of technologies to ensure data protection is critical. Best in Class companies strongly prefer end to end data protection and layer their defense.

### Case Study: A Leading Bank in the Global 2000

"Banks are where the money is." quips an IT manager in the Global 2000. "We're easy targets, and despite best efforts, things are getting worse. The attacks are more sophisticated, more targeted."

"Our strategy is a layered defense with no single point of failure, but you have to remember the human element. Eighty percent of security breaches are by staff and 80% are non-malicious in nature." That being said he recommends that all email be encrypted and that all paper records be shredded. "When we have technology that can sit in the background and scan for personally identifiable information in email, take action to encrypt it, and have it easily unencrypted by the receiver, every company should be using it."

The bank uses encryption, enterprise rights management, firewalls, anti-phishing/anti-spyware software, data loss prevention software, and web filtering. Asked what he would do differently with an unlimited budget, he replied "Send the entire C-level staff to 'Scared Straight Boot Camp'. Until we do, customers, stockholders, the business itself and our careers are all at extreme risk."

### Fast Facts

- √ Best-in-class companies are almost **twice as likely** as the rest to train their users in appropriate data use and compliance requirements.
- √ Best-in-Class are **more than twice as likely** as Industry Laggards to use Data Loss Prevention Software.

The top three strategies identified by Best in Class companies are:

- Identify and protect sensitive data (77%)
- Attain regulatory compliance (58%)
- Deploy end-to-end data protection (58%)

## Competitive Assessment

Survey respondents fall into one of three categories – Laggard, Industry Average, or Best in Class — based on their characteristics in five key categories: (1) process (auditing data use); (2) organization (training users on appropriate data use and compliance requirements); (3) knowledge (monitoring data use and real-time notification of data use); (4) technology (using technologies specific to preventing data loss); and (5) performance management (success in protecting sensitive data from insider threats).

**Table 3: Competitive Framework**

	Laggards	Average	Best in Class
Process	Auditing data use		
	20%	41%	56%
Organization	Train users in data use and compliance requirements		
	25%	40%	52%
Knowledge	Monitor data use		
	22%	46%	52%
	Real-time notification of inappropriate data use		
	3%	16%	28%
Technology	Data / information loss prevention technology in use		
	17%	21%	40%
Performance	96-100% of sensitive data protected from insider threat		
	0%	0%	31%

Best-in-Class companies' strong preference for end-to-end data protection and attaining regulatory compliance is evidenced in their process, organizational action, use of critical information and enabling technologies.

Source: Aberdeen Group, May 2007

### **Organizational Capabilities and Technology Enablers**

Across the board, the companies surveyed are employing elements of data protection – encryption, firewalls, web-filtering, anti-phishing / pharming / spyware solutions – at roughly the same rate, with Best in Class a little over 6% better penetrated. The most noticeable differences are in their use of:

- Data loss prevention software (Best in Class is nearly twice as likely as others to already be using data loss prevention software)
- Data use auditing (the Best in Class are 15% more likely to audit their data use)
- Real-time notification of inappropriate data use (Best in Class are almost twice as likely to use real-time notification)

However, even Best in Class companies have a ways to go to ensure that their data is safe. In asking end-users what is hampering their efforts to secure their sensitive data two serious issues arise:

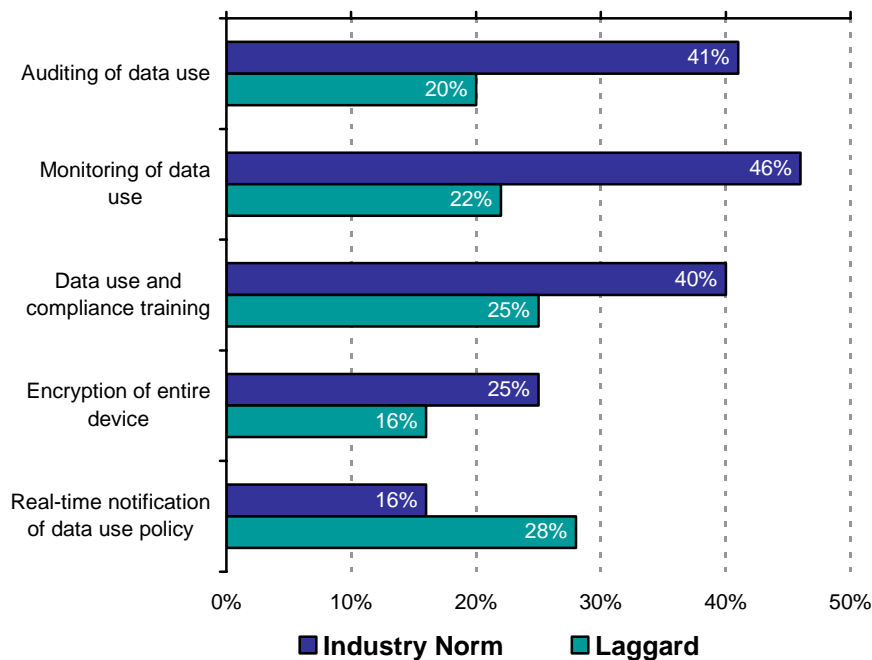
- A lack of understanding and support from executive management. Despite media attention to the problems caused by

stolen and lost laptops, the hawking of proprietary information, and the damage caused by disgruntled employees, without management commitment to the changes in process that may be necessary to effect data security, simply implementing appropriate technologies will not be enough. Even the creation of policies is insufficient if management doesn't insist on enforcing policies and following through with consequences for policy breach.

- A lack of training and understanding of appropriate data use. Until an organization assesses its data risk, creates the necessary policies and teaches people what constitutes appropriate (and inappropriate) use, sensitive data will not be protected.

Most concerning are the companies who neither know nor measure how much of their sensitive data is protected, nor how many data breaches they experience, nor the extent of their financial loss as the result of data breaches. These same companies lag the market in adoption of appropriate technologies and are at greater risk.

**Figure 4: Technology Adoption in Laggards vs. Industry Norm**



Source: Aberdeen Group, May 2007

### Aberdeen Insights – Technology

Protecting sensitive data requires an actual strategy that includes an assessment of what constitutes sensitive data for your organization, discovering where sensitive data resides, classifying the data as sensitive and protecting the sensitive data – while it's at rest ( stored somewhere) while it's in motion (across a network), and while it's in use (by an application). Simultaneously, protecting sensitive data must not hinder an organization's ability to do business. And organizations, people, projects and roles change, meaning that organizations have to think through policies for data usage, roles and rules for roles.

To deploy an end-to-end data protection policy requires vision and leadership from senior management. Asking an industry veteran charged with data protection for a large financial institution why successfully protecting data is so difficult, the reply came "Senior level management isn't paying attention. The right people are ignorant of what it takes. Until senior management is truly held accountable, things won't change. Management needs to take some hard, unpopular steps."

## Chapter Three: Required Actions

Whether a company is trying to move its performance in data protection from “Laggard” to “Industry Average,” or “Industry Average” to “Best in Class,” the following actions will help spur the necessary performance improvements:

### Laggard Steps to Success

---

- Make data protection a top priority – only 3% of the Laggard companies view data protection / information loss prevention as a top 2 priority verses 23% of the Best in Class. Until data loss prevention is given the attention it warrants, companies persist in putting themselves at risk.
- Use data loss prevention software and auditing software to monitor, know and document who’s using your data and how.
- Define data use policies, train employees in appropriate data use, and actively notify users of inappropriate data use. Inappropriate data use will show up in monitoring and log data, but data loss prevention software that notices that a user is trying to perform a questionable action and notifies that user – either preventing the action, simply alerting the user or asking users to acknowledge their actions by confirming that they indeed are trying to do what the system is alerting them to. In this way, policy can be enforced; users learn appropriate and inappropriate data use, and high risk behavior is acknowledged.

### Industry Norm Steps to Success

---

- Perform a risk assessment either internally or using external consultants to determine what data needs protection
- Create policy for data use specifying who has what kind of access under what conditions
- Use data loss prevention and auditing technologies to monitor, audit and enforce data use policies
- Implement data loss prevention software with real-time notification to alert users to inappropriate or potentially inappropriate data use.

### Best in Class Steps to Success

---

- Use automated discovery to identify, classify and protect sensitive data. Sixty-nine percent of Best in Class companies protect less than 96% of their sensitive data, some reporting data breach incidents resulting in losses greater than \$1,000,000. Without automated discovery, organizations may never find where all their sensitive data resides. The use of automated discovery capability is one significant component of data loss prevention solutions – a key differentiator evidenced in its use by Best in Class companies.

#### Fast Facts

- 98% of Best-in-class companies say that the discovery of confidential information on their systems is important or very important.
- 94% of Best-in-class companies say the ability to configure policies for data use is important or very important.

- Hold everyone accountable for appropriate data use. After appropriate training, insist on appropriate data use with consequences for inappropriate data use.
- Supplement internal monitoring and auditing of data use with third party, independent audit.

#### Aberdeen Insights – Summary

Securing sensitive data requires an all-out determined initiative. It requires identifying and classifying data as sensitive and putting policies in place to protect it. These policies may well impact organizational process and may have a negative impact on user productivity in some instances, so it behooves an organization to give careful thought to exactly what policies are necessary and how best to implement them.

Best-in-class companies appear to benefit by holding themselves accountable to external compliance regulations. It's interesting to think that although compliance regulations are put in place to hold organizations accountable for protecting sensitive information (HIPAA protecting patient information, SOX protecting financial information, for example), the organizations themselves benefit directly by suffering fewer breaches and less financial loss. Without making regulatory compliance a stated goal, companies are not gaining ground against the rise in data breach incidents. As attacks are automated and become more and more sophisticated, those organizations that do not protect themselves become even more vulnerable.

The work needed to secure sensitive data is ongoing. Companies need to begin by assessing their risk and determining where their sensitive data resides. They need policies and ways of enforcing those policies. Companies that are automating the discovery of sensitive data at rest and the detection of sensitive data in motion are making strides toward securing it. Determining data use policy and teaching people how to handle sensitive data is critical to the ultimate success of any data protection strategy. Without a strong data protection strategy organizations remain at risk.

[Send to a Friend](#) 

## Appendix A: Research Methodology

Between April and May 2007, Aberdeen Group examined the use of data protection / data loss prevention technologies and experiences of more than 150 organizations across a spectrum of industries.

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

- The strategies and technologies in use to prevent data loss, and the effectiveness of these strategies and technologies
- The progress (or lack there of) in effectively reducing or eliminating data breaches
- The importance of particular capabilities in their battle against data loss

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

The study aimed to identify emerging best practices for data loss prevention and provide a framework by which readers can assess their own management capabilities.

Responding enterprises included the following:

- **Job title/function:** The research sample included respondents with the following job titles: IT manager or staff (25%); director (22%); senior management (CEO, COO, CFO, president, vice president) (21%); CIO (15%); other (9%); consultant (8%).
- **Industry:** The research sample included respondents across industries. High tech and software companies represent 18% of the sample. Finance, banking and accounting represent 12%; healthcare / medical services and products represent 11%. Public sector organizations represent 9%. The remaining respondents span all industries including aerospace, telecommunications, manufacturing, publishing and transportation.
- **Geography:** The majority of respondents (78%) were from North America. Remaining respondents were from Europe (10%) the Asia-Pacific region (7%), and South/Central America and Caribbean (5%).
- **Company size:** 19% of respondents were from large enterprises (annual revenues above US\$1 billion); 26% were from midsize enterprises (annual revenues between \$50 million and \$1 billion); and 55% of respondents were from small businesses (annual revenues of \$50 million or less).

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

**Table 4: PACE Framework**

**PACE Key**

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, May 2007

**Table 5: Maturity Framework**

**Maturity Framework Key**

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

**Best in class (20%)** — Companies that are protecting a large share of their sensitive data against both insider and external threats, and are reducing the number of data breaches they experience.

**Industry norm (50%)** — Companies that represent the average or norm, and result in average industry performance.

**Laggards (30%)** — Companies 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, May 2007

**Table 6: Relationship between PACE and Competitive Framework**

**PACE and Competitive Framework How They Interact**

Aberdeen research indicates that companies that identify the most impactful pressures and take the most transformational and effective actions are most likely to achieve superior performance. The level of competitive performance that a company achieves is strongly determined by the PACE choices that they make and how well they execute.

Source: Aberdeen Group, May 2007

## **Appendix B: Related Aberdeen Research**

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

- [\*Identity and Access Management Critical to Operations and Security\*](#), March 2007
- [\*The Endpoint Security Strategies Part II: The Data Protection Benchmark\*](#), December 2006

Information on these and any other Aberdeen publications can be found at [www.Aberdeen.com](http://www.Aberdeen.com).

Carol Baroudi, Research Director, Security [carol.baroudi@aberdeen.com](mailto:carol.baroudi@aberdeen.com)

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

This document is the result of research performed by Aberdeen Group. Aberdeen Group believes its findings are objective and represent the best analysis available at the time of publication. Unless otherwise noted, the entire contents of this publication are copyrighted by Aberdeen Group, Inc. and may not be reproduced, stored in a retrieval system, or transmitted in any form or by any means without prior written consent by Aberdeen Group, Inc.