Aberdeen Group
A Harte-Hanks Company

Send to a Friend

Trusted Computing

Tune In, Turn it On

February 2008

Aberdeen Group
A Harte-Hanks Company

Executive Summary

This research benchmark provides insight and recommendations for all organizations that are interested in decreasing their reliance on software-based security solutions and learning more about the benefits of **trusted computing** solutions, which leverage hardware-based "roots of trust" at the edge of the network and at the endpoints.

Best-in-Class Performance

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

- Number of security-related incidents
- Number of non-compliance incidents (e.g., failed audits)
- Amount of human error related to security
- Ongoing management costs related to security

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

Competitive Maturity Assessment

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

- 89% implemented consistent security and compliance policies across the enterprise
- 70% conducted formal risk assessments
- 68% developed systematic implementation / roll out processes for security solutions
- 68% developed standardized audit, analysis, and reporting for security and compliance
- 63% prioritized their objectives for security controls as a function of risk, audit, and compliance requirements

Recommended Actions

In addition to the specific recommendations in Chapter Three of this report, to achieve Best-in-Class performance companies should increase their awareness about the capabilities of the trusted computing model and security solutions that leverage Trusted Platform Modules (TPM), and identify applications that take advantage of the trusted computing-ready devices and infrastructure that already exists within their enterprise.

Send to a Friend

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 anticipation of emerging encryption product capabilities as well as requirements for device authentication, DOD Components shall ensure all new computer assets (eg, server, desktop, laptop, and PDA) produced to support the DOD enterprise include a Trusted Platform Module version 1.2 oe higher where such technology is available."

~US DOD Memorandum, Article 4, July 2007

"What's a TPM?"

~ IT Security Director, Global 1000 Company

© 2008 Aberdeen Group.

Aberdeen Group
A Harte-Hanks Company

Table of Contents

Figures

Tables

© 2008 Aberdeen Group.

Aberdeen Group
A Harte-Hanks Company

Chapter One: Benchmarking the Best-in-Class

Business Context - What is Trusted Computing?

In his acceptance speech for the 1983 Turing Award, Ken Thompson (who was recognized along with Dennis Ritchie for their contributions as the principal creators of the Unix operating system) famously remarked: "The moral is obvious. You can't trust code that you did not totally create yourself. (Especially code from companies that employ people like me.)"

Twenty-five years later, the awareness that software is untrusted is pervasive. Programs are vulnerable due to coding defects, buffer overflows, and parsing errors. Systems are vulnerable to trojans and other malware. Servers, devices and endpoints are vulnerable for being misconfigured and unpatched, in spite of a never-ending treadmill of "patch Tuesdays."

Heightened lack of trust in software is at the heart of a different approach to IT security, known as *trusted computing*. The core idea behind trusted computing is to leverage hardware-based "roots of trust" at the edge of the network and at the endpoints – what some refer to as "hardware anchors in a sea of untrusted software" – for higher assurance.

Security solutions which rely on these hardware-based roots of trust are therefore not merely new (untrusted) software layered on top of existing (untrusted) software. Industry-leading vendors have collaborated to define standards for these hardware-based roots of trust, which are inherently more secure from external software attack and physical theft than software-only implementations. On-chip security operations, which are executed in a closed hardware environment, include:

- Public-key cryptographic functions – such as key pair generation, random number generation, digital signature and verification of digital signatures, and encryption / decryption
- Integrity measurement functions – to protect data (such as private keys) from access by malicious code
- Attestation functions – to provide cryptographic proof to a third-party that software has not been compromised

Over the past several years, leading solution providers have been embedding the hardware and software building blocks for trusted computing (such as the standard Trusted Platform Module chip, or TPM) into their off-the-shelf, enterprise-class offerings. Examples of security applications which can be enhanced by leveraging the hardware-based building blocks of trusted computing within existing systems include:

- PCs (clients) - pre-boot authentication, Windows log-on, endpoint security, user authentication, device authentication
- Servers - device authentication

Fast Facts

√ 12% of all respondents indicated that they have deferred trusted computing initiatives based on the upgrade / replacement cycles for TPM-compatible solutions

√ 20% of all respondents expressed concerns about standards being perceived as lacking or immature

© 2008 Aberdeen Group.

- Mobile devices (smart phones, PDAs) - endpoint security, user authentication, device authentication
- Hard drives, storage systems - hardware-based encryption and key management
- Network security - ensures that endpoints are in compliance with security policies at, and after, connection to the network
- Hardcopy devices (printers) - secure printing services

Because these capabilities are embedded directly within new enterprise-class systems, they have been and continue to be rolled out as part of the natural enterprise acquisition and replacement cycles. The foundation is being put in place, and in many cases it is already there.

When trusted computing emerged just a few years ago, there was a considerable amount of suspicion aroused by an industry-led initiative. Microsoft's "Palladium" and Sony's attempt to bundle music-protection software (which was essentially a rootkit) on new CDs created considerable public outcry, such as Richard Stallman's position about "trusted" actually meaning "treacherous." Even in 2007, a short video questioning the merits of trusted computing for consumers won a production award from Adobe (and is still available on YouTube). The biggest concerns seem to be about the degree of control held by the content creators (licensors) versus control held by the content users (licensees).

This benchmark study deals explicitly with trusted computing in the context of the enterprise, where the assumption is that the enterprise (not the end-user) owns the endpoints. The matter of trusted computing in the context of endpoints owned by the consumer is not addressed in this study.

"It's interesting ... there really isn't a lot of in-your-face marketing about the benefits of trusted computing and the TPM. It's surprising to me that more people don't just include this in their procurement."

~ Network Security Manager, Mid-sized Retail Franchise

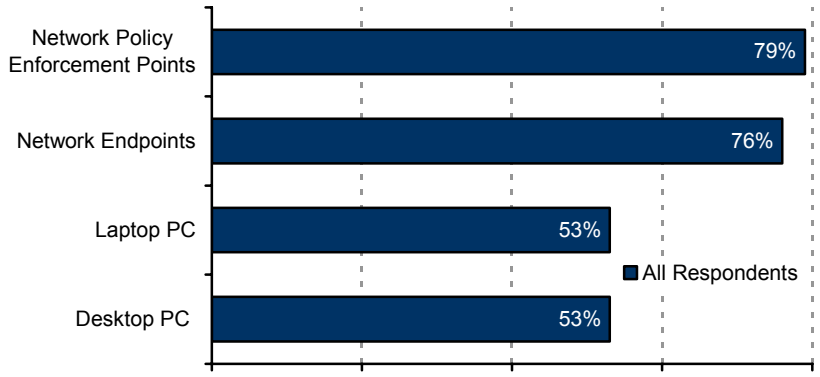
Two important findings of this study are:

- Enterprise awareness about trusted computing and TPM is still relatively low
- A high percentage of trusted computing-ready devices and infrastructure within the enterprise already exists

Both of these findings speak to the need for more education. The average percentage of PCs and network devices identified by survey respondents as being able to support trusted computing is shown in Figure 1. Respondents in this study estimated that more than half of existing desktop PCs and laptop PCs already had support for trusted computing. In addition, they estimated that more than three-fourths of existing network endpoints and policy enforcement points can support trusted computing as currently deployed.

© 2008 Aberdeen Group.

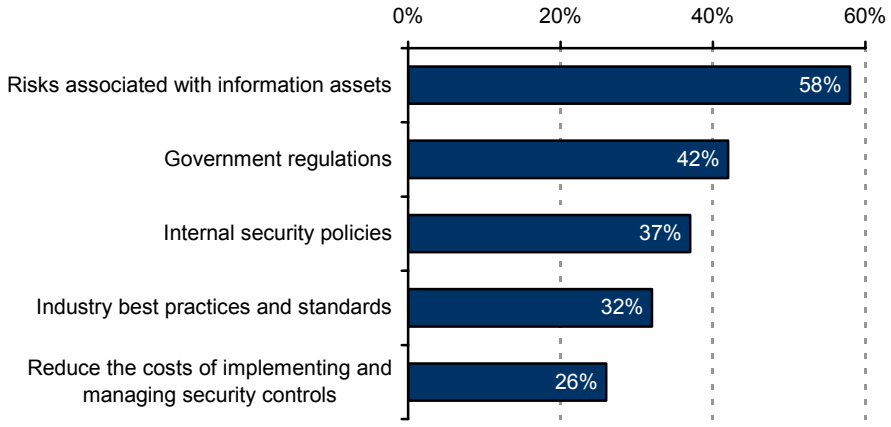
Figure 1: Existing Systems with Support for Trusted Computing



Source: Aberdeen Group, February 2008

The top pressures driving organizations to focus resources on implementing or evaluating trusted computing initiatives are those we have seen in virtually all security benchmark studies over the past year. Risks, regulations, internal policies, and industry best practices and standards continue to be the leading market drivers (Figure 2).

Figure 2: Leading Drivers for Trusted Computing Initiatives



Source: Aberdeen Group, February 2008

The exception in this study is "reduce the costs of implementing and managing security controls," which is a more recently emerging theme. In Aberdeen's November 2007 research on *Security Governance and Risk Management*, clear evidence is presented that companies with leading performance are taking proactive steps to ensure that their investments in security and compliance controls directly support their strategic objectives for the business, although their capabilities in this regard are still developing. Many organizations believe their current levels of investment in security and compliance have gotten out of balance, taking an increasing share of limited IT resources – and effectively constraining the organization's ability to deliver new products and services. Rather than sustain spending on security

© 2008 Aberdeen Group.

and compliance for its own sake, Best-in-Class organizations have begun to develop security Governance, Risk management and Compliance (GRC) processes to more effectively allocate their IT resources and activities based on business objectives and acceptable levels of risk.

The Maturity Class Framework

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

- Number of security-related incidents
- Number of non-compliance incidents (e.g., failed audits)
- Amount of human error related to security
- Ongoing management costs related to security

Companies with top performance based on these criteria earned Best-in-Class status, as described in Table 1. (For additional details on the Aberdeen Maturity Class Framework, see Table 5 in Appendix A.) Survey responses from over 100 organizations representing a diverse set of industries are included in this study.

Table 1: Top Performers Earn Best-in-Class Status

Definition of Maturity Class	Mean Class Performance
Best-in-Class: **Top 20%** of aggregate performance scorers	▪ 74% **decreased** the number of actual security-related incidents in the last 12 months ▪ 48% **decreased** the number of non-compliance incidents (e.g., failed audits) ▪ 63% **reduced** the amount of human error related to security ▪ 0% increased the ongoing management costs related to security
Industry Average: **Middle 50%** of aggregate performance scorers	▪ 7% **decreased** the number of actual security-related incidents in the last 12 months ▪ 3% **increased** the number of non-compliance incidents (e.g., failed audits ▪ 0% reduced the amount of human error related to security ▪ 32% **increased** the ongoing management costs related to security
Laggard: **Bottom 30%** of aggregate performance scorers	▪ 58% **increased** the number of actual security-related incidents in the last 12 months ▪ 60% **increased** the number of non-compliance incidents (e.g., failed audits) ▪ 71% **increased** the amount of human error related to security ▪ 95% **increased** the ongoing management costs related to security

Note: Percentages shown are the net of "increased," "stayed the same," and "decreased"
Source: Aberdeen Group, February 2008

The Best-in-Class PACE Model

Using the building blocks of trusted computing to enhance enterprise security 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

© 2008 Aberdeen Group.

Framework, see Table 4 in Appendix A). The characteristics exhibited by Best-in-Class organizations in this study are summarized in Table 2.

Table 2: The Best-in-Class PACE Framework

Pressures	Actions	Capabilities	Enablers
▪ Risks associated with information assets	▪ Develop a holistic view of security risks across the organization ▪ Establish and enforce consistent security policies and procedures across the organization ▪ Protect data at rest and in motion ▪ Ensure that devices accessing the network comply with policy	▪ Consistent security and compliance policies ▪ Formal risk assessments ▪ Systematic implementation / roll out processes for security solutions ▪ Standardized audit, analysis, and reporting ▪ Security control objectives prioritized as a function of risk, audit, and compliance requirements ▪ Responsible executive or team with primary ownership for security risk ▪ Formal documentation, awareness, and end-user training programs around security ▪ Clear mapping of risks and controls to the various regulations, standards, policies, and best practices to which they relate ▪ Controls to monitor and verify that requirements of internal policies and external regulations are being satisfied ▪ Identification of all information required for auditing and reporting ▪ Monitor security of information assets ▪ Monitor security of physical assets	▪ Network Access Control (NAC) ▪ Data Encryption ▪ Identity & Access Management (IAM) ▪ Configuration and Change Management ▪ Trusted Platform Modules (TPM)

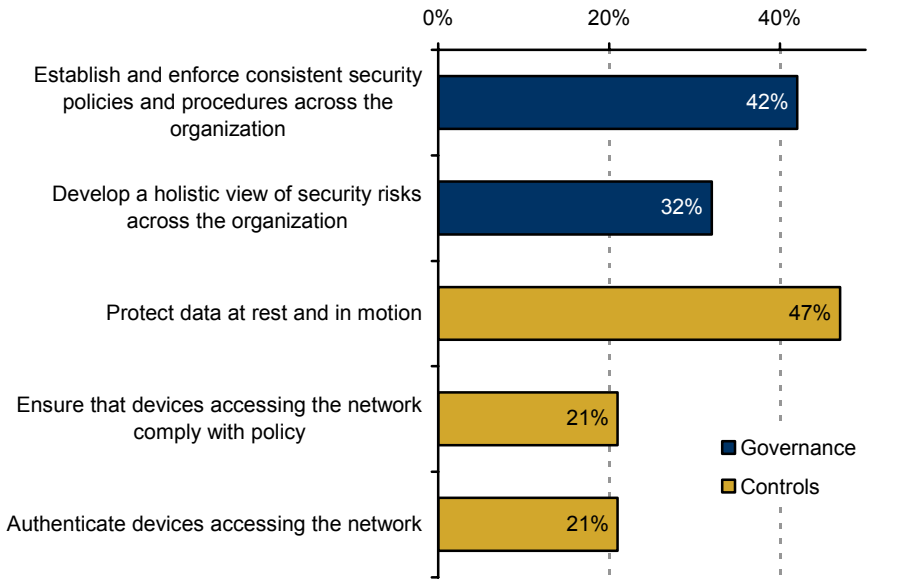
Source: Aberdeen Group, February 2008

Best-in-Class Strategies

Policy-driven, risk-driven strategies correlate most highly with current investments in trusted computing initiatives. Across several of our recent security benchmark reports, "develop a wholistic view of security risks" and "establish and enforce consistent security policies" across the organization are top strategies for Best-in-Class organizations. In addition, data protection and network access are two classes of solution that rank highest as strategic drivers (Figure 3).

© 2008 Aberdeen Group.

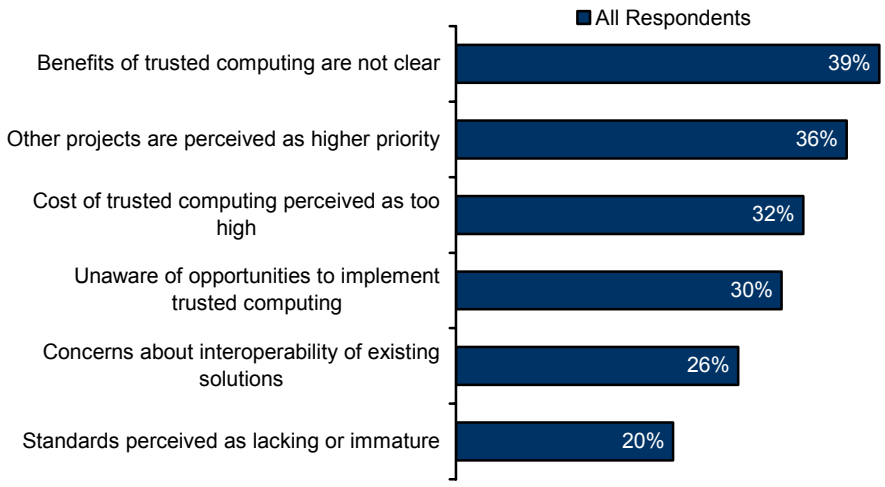
Figure 3: Best-in-Class Strategies Driving Current Investments



Source: Aberdeen Group, February 2008

When asked about top reasons their organization had *not* invested in trusted computing initiatives, respondents identified "benefits are not clear," "other projects are perceived as higher priority," "cost perceived as too high," and "unaware of opportunities to implement" as the leading barriers to adoption (Figure 4). Given that Best-in-Class organizations in this study have improved security and compliance, reduced human error (e.g., through automation), and held the line on ongoing operating costs, Figure 4 underscores the importance of increasing education and awareness about the opportunities and benefits of trusted computing in the enterprise.

Figure 4: Leading Barriers to Adoption - Education and Awareness



Source: Aberdeen Group, February 2008

© 2008 Aberdeen Group.

In the next chapter, we will see what the top performers are doing to achieve these gains. We also examine the capabilities of current TPM users in comparison to other respondents in the study.

Aberdeen Insights – Strategy

Awareness continues to grow that "trusted computing" is based on a fundamentally different philosophical approach:

- Traditional security solutions are based on a "black list" model – security is peripheral to the main design of the application, and the general approach is to identify what's bad as quickly as possible and to prevent the bad things from happening.
- Trusted computing solutions are based on a "white list" model – security is based on defining behavior that is allowed, and the general approach is that once "healthy" behavior has been defined, all variants are deemed "unhealthy" and are not allowed.

In other words, trusted computing represents the "built in" versus "bolted on" approach to security that industry leaders have been talking about for the last several years.

It is still early for trusted computing deployments, but the research provides strong evidence that an inflection point is quickly approaching. The threat landscape is constantly evolving, and the software-based arms race – between the makers of software-based threats, and the makers of software-based solutions designed to protect against those threats – continues to escalate. The result is ever-increasing spend on security and compliance, and for the Industry Average the data consistently shows a "treading water" kind of result. These levels of investment without results cannot be sustained. Much like Homeland Security, the challenge with the perimeter / black list approach is that the evildoers have to succeed only once, whereas the defenders have to succeed 100% of the time.

Education and awareness about the immediate opportunities provided by existing trusted computing infrastructure is the first critical step. The research shows that enterprise security can be enhanced, using the building blocks that are already there, and improvements can be layered on incrementally over time. Large scale rip-and-replace investments are not required, and organizations need not wait for complete turnover of their IT infrastructure (which is typically three years or more). Strategically, the goal remains a consistent, enterprise-wide approach to security, risk management and compliance, but best practice is to build success one project at a time.

The trusted computing infrastructure that has been shipping into the enterprise for the last few years was designed around an "opt-in" model, giving the enterprise full control. To make it work for you, you have to turn it on.

Fast Facts

How long current TPM-based security solutions have been in place:

√ More than 24 months (54%)

√ 12 to 24 months (13%)

√ 6 to 12 months (4%)

√ Less than than 6 months (8%)

√ Rolling out over the next 12 months (17%)

√ Pilot / evaluation (4%)

© 2008 Aberdeen Group.

Aberdeen Group
A Harte-Hanks Company

Chapter Two:
Benchmarking Requirements for Success

The selection of specific opportunities to roll out trusted computing applications – and the policy, planning, process, and organizational elements of implementation – are critical success factors in the ability to realize the business benefits of better security, sustained compliance, reduced human error, and lower cost of ongoing management.

Case Study – Papa Gino's, Dedham, MA

Papa Gino's is New England's leading quick-service Italian restaurant chain, specializing in American-style pizza, pasta, subs, and salads. With headquarters in Dedham, Massachusetts, Papa Gino's has nearly 170 locations in Connecticut, Maine, Massachusetts, New Hampshire, and Rhode Island. The company, which also operates over 200 D'Angelo Grilled Sandwiches restaurants, serves more than 13 million guests annually.

Their journey on the path of trusted computing began during the proposal process for new point-of-sale systems, when Chris Cahalin, network security manager at Papa Gino's, uncovered information on enhanced security and trusted computing on the vendor web site. "Our budgets are tight, and we really can't afford to make a mistake," says Cahalin. "So I want to make sure that the equipment and solutions we bring in are going to last a while. The work Microsoft was doing at the time with the next-generation secure computing base told me that software alone wasn't enough, and told me to keep an eye on the hardware."

The vendor's sales rep was quick to bring in resources that could speak to trusted computing, and ultimately Papa Gino's selected PCs with TPM capabilities. The initial trusted computing application was file / folder encryption to protect financial information. This had been a problem in the past, when lost encryption keys meant losing access to the financial data at an especially critical time: the end of a fiscal year. By using the TPM, all information placed in designated folders was automatically encrypted, and the keys were automatically backed up. "If I ever had to get at the data, there's a standard audited process to do that," notes Cahalin. "For the first time, we had tangible control over our security environment."

continued

© 2008 Aberdeen Group.

Aberdeen Group
A Harte-Hanks Company

Case Study – Papa Gino's, Dedham, MA

The use of trusted computing for data protection has expanded over time. "Full-disk encryption is now a standard order for us. The self-encrypting hard drives can also be centrally managed." Cahalin notes that the new solutions provide centralized control at a very granular level, for example to decide that a particular user should no longer have access to the data, or to remotely repurpose a PC through "instantaneous cryptographic shredding."

Papa Gino's has subsequently leveraged the TPM for user authentication, for example using a finger-swipe biometric for pre-boot authentication and for logging on to Windows. Enhancing the security of network access is next on the list, and Cahalin is currently talking with a short list of vendors for this application. "One of the ways we can protect the network is to ensure that only the employee can authenticate to the device, and then release a TPM-housed digital certificate to authenticate to the network."

Papa Gino's is an excellent illustration of first tuning in to the enhanced security made possible by trusted computing infrastructure, then selectively turning it on by implementing TPM-enabled applications over time as new systems are deployed and as IT resources are available. "We're a pizza shop," comments Cahalin. "We're slow and steady. We just keep rolling stuff out."

Competitive Assessment

Aberdeen analyzed the aggregated metrics of surveyed companies to determine whether their performance ranked as Best-in-Class, Industry Average, or Laggard.

In addition to having common levels of performance, each maturity class also shared common characteristics in five categories:

1. **Process**. The approaches taken to execute daily operations
2. **Organization**. Corporate focus and collaboration among stakeholders
3. **Knowledge management**. Putting data in context and exposing it to key stakeholders
4. **Technology**. The selection of appropriate tools, and the effective deployment of those tools
5. **Performance management**. The ability of the organization to measure results to improve the business

These characteristics, identified in Table 3, serve as a guideline for best practices, and correlate directly with Best-in-Class performance across the associated metrics.

© 2008 Aberdeen Group.

Aberdeen Group
A Harte-Hanks Company

Table 3: Competitive Framework

	Best-in-Class	Industry Average	Laggards
Process	Consistent security and compliance policies		
	89%	74%	48%
	Formal risk assessments		
	70%	68%	64%
	Systematic implementation / roll out processes for security solutions		
	68%	50%	38%
	Standardized audit, analysis and reporting		
	68%	55%	48%
	Security control objectives prioritized as a function of risk, audit and compliance requirements		
	63%	56%	51%
Organization	Responsible executive or team with primary ownership for security risk		
	79%	74%	68%
	Formal documentation, awareness and end-user training programs around security		
	68%	57%	50%
Knowledge	Clear mapping of risks and controls to the various regulations, standards, policies and best practices to which they relate		
	63%	44%	40%
Technology	Controls to monitor and verify that requirements of internal policies and external regulations are being satisfied		
	59%	53%	52%
	Security technologies currently in use (also see Figure 6)		
	▪ NAC 74% ▪ IAM 74% ▪ Configuration and change management 72% ▪ Data encryption 72% ▪ TPM 39%	▪ NAC 60% ▪ IAM 58% ▪ Configuration and change management 70% ▪ Data encryption 70% ▪ TPM 30%	▪ NAC 50% ▪ IAM 50% ▪ Configuration and change management 65% ▪ Data encryption 67% ▪ TPM 22%
Performance	Identification of all information required for auditing and reporting		
	68%	51%	50%
	Monitor security of information assets		
	68%	65%	50%
	Monitor security of physical assets		
	84%	62%	58%

Source: Aberdeen Group, February 2008

© 2008 Aberdeen Group.

Capabilities and Enablers

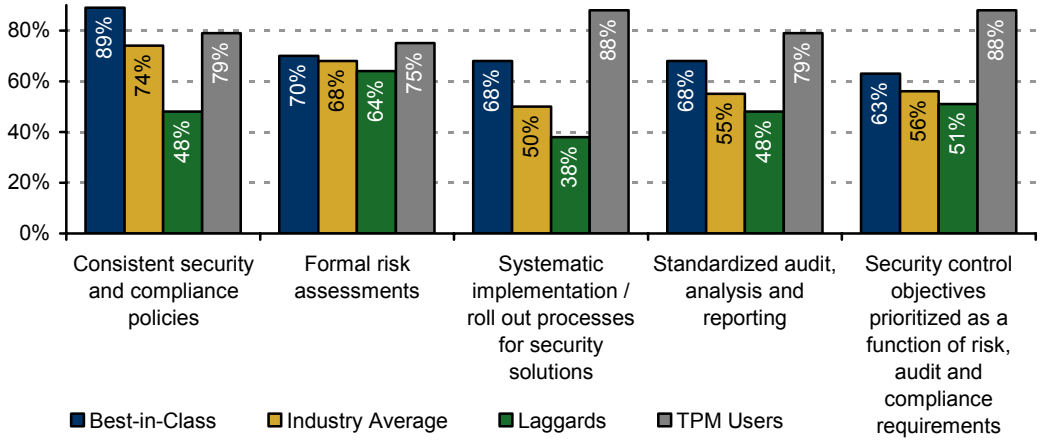
Based on the comparisons within the Competitive Framework and interviews with select end-user organizations, analysis of the Best-in-Class highlights the degree to which they have developed their security-related business processes beyond those of their Industry Average and Laggard counterparts. An analysis of current users of TPM-based solutions, however, shows that **TPM users exhibit superior capabilities in all five categories** of Aberdeen's PACE model.

Process

Compared to the other maturity classes, the Best-in-Class have developed more systematic, sustainable business processes around security and compliance. In this study they were 90% more likely than Laggards to have consistent security and compliance policies, the bedrock of success for security governance, risk management, and compliance. In addition, they were 80% more likely than Laggards to have systematic implementation and rollout processes for their security solutions (Figure 5).

Figure 5 also demonstrates that current TPM users have developed outstanding process capabilities, in most cases even superior to those of the Best-in-Class. They have prioritized objectives for their security controls as a function of risk, audit, and compliance requirements. They have established consistent policies, and have standardized requirements for audit, analysis and reporting. They have developed more systematic processes to roll out security solutions across the enterprise. As our previous research has repeatedly shown, tactical deployment of point solutions where specific needs exist is currently the market norm, but the more centralized control provided by TPM-based solutions aligns extremely well with the Best-in-Class practice of taking a more strategic, enterprise-wide approach.

Figure 5: TPM Users Exhibit Superior Process Capabilities



Source: Aberdeen Group, February 2008

© 2008 Aberdeen Group.

Aberdeen Group
A Harte-Hanks Company

Organization

As seen in Table 3, Best-in-Class organizations not only have clear ownership for security and risk by an executive or team, but also have invested in documentation, awareness and training for end-users around security. Current TPM users, however, have developed these capabilities to a higher degree at both ends. In this study, 92% of current TPM users have a responsible executive or team with ownership for security and risk, and 88% have invested in formal documentation, awareness, and end-user training. The standard processes and consistent policies established by TPM users, as discussed earlier, certainly make it easier to educate end-users on expected and acceptable behavior.

"We think the mark of a secure system is where you have enhanced security and higher assurance, but end-users don't really see it as out of the ordinary in the way they go about their daily tasks."

~ CIO, Small Enterprise

Knowledge Management

Current TPM users (79%) are nearly two-times as likely as Laggards (40%) to have a clear mapping of risks and controls to the various regulations, standards, policies, and best practices to which they relate. By definition, they have proactively and purposefully turned on TPM-enabled applications to enhance IT security, as opposed to deploying solutions willy-nilly in a series of tactical responses to the most recent problems.

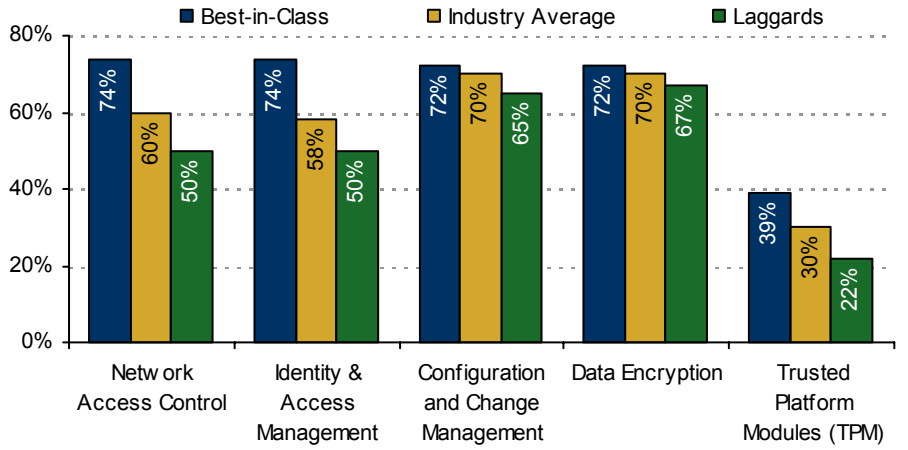
Technology

Best-in-Class organizations have developed a slightly stronger alignment between their policies and their technical controls, compared to Industry Average and Laggards (Table 3). Over 70% of current TPM users, however, report having controls in place to monitor and verify that the requirements of internal policies and external regulations are being fully satisfied.

Selected enterprise security technologies currently deployed are shown in Figure 6. In this study, Best-in-Class organizations have deployed network access control and identity management solutions at about 1.5-times the rate of Laggards. They are also 80% more likely to have deployed TPM-based solutions, although at only 39% we see that it is still early for turning on the capabilities made possible by the trusted computing infrastructure. In previous studies, between 11% and 15% of all respondents have indicated current support for TPM-based solutions.

© 2008 Aberdeen Group.

Figure 6: Enterprise Security Technologies Currently Deployed



Source: Aberdeen Group, February 2008

What applications have current TPM users enabled? Based on the research, the most common deployments fall into three broad categories:

Network access:

- Network Access Control (NAC / NAP / TNC) - 75% of current TPM users
- Wireless network access (802.1x) - 74%
- Remote network access (IPSec VPN) - 74%
- Device authentication - 71%
- Device attestation (e.g., "posture" / "health") - 48%

Data protection:

- Full-disk encryption - 67% of current TPM users
- File / folder encryption - 63%
- Encryption key management - 54%
- Secure email - 75%

User authentication:

- Secure boot sequence - 79% of current TPM users
- PC login - 88%
- User authentication - 83%
- Smart cards - 45%
- Fingerprint biometrics - 39%

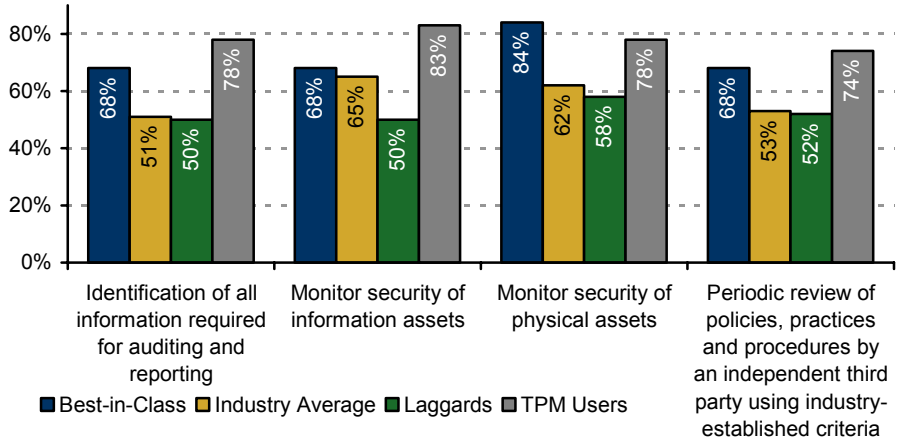
© 2008 Aberdeen Group.

Appendix B provides pointers to three related Research Briefs, each based on this *trusted computing* study, with additional detail on trusted computing and network access, data protection, and user authentication, respectively.

Performance Management

Best-in-Class organizations have identified the information required for auditing and reporting, and are better at monitoring to ensure the security of their corporate assets. Current TPM users have also developed exceptionally strong current capabilities in these areas (Figure 7).

Figure 7: TPM Users Exhibit Superior Performance Management



Source: Aberdeen Group, February 2008

Aberdeen Insights — Technology

Trusted computing infrastructure has steadily become more prevalent in the enterprise, but turning on the TPM is by design done on an opt-in basis. By definition, current TPM users are deliberate and purposeful in their approach to enhancing enterprise security, and the research shows that they are also more disciplined in their capabilities. This leads not only to better security and sustained compliance initiatives, but also to reduced human error and lower cost of ongoing management.

Based on the research, the leading areas to get started in trusted computing are network access, data protection, and user authentication:

Network access. Network access solutions can leverage TPMs and standards such as 802.1x to enhance security in both the wired and wireless worlds. Concerns about interoperability have lessened in the last year, as a result of cross-licensing agreements between leading industry players and the ongoing maturation of the industry-led standards and interoperability process.

continued

© 2008 Aberdeen Group.

Aberdeen Group
A Harte-Hanks Company

Aberdeen Insights — Technology

TPMs can be leveraged in several ways in the context of secure network access: authenticating users; authenticating devices; and verifying compliance of software at the endpoints (e.g., the integrity of client-side software such as the BIOS, the operating system, drivers, anti-virus) and the identification of rootkits. The security operations team is increasingly becoming educated that the network itself can provide an additional layer of defense, by stopping the bad bits from reaching the network in the first place. In addition, mechanisms such as 802.1x can associate a set of privileges and quality of service based on where network log on occurs, without requiring the network operations team to take on burdensome reconfigurations. Still, there are enough moving parts that leveraging TPM and / or 802.1x in increments is a practical and successful approach.

Data protection. Storage presents a significant opportunity to leverage the principles of trusted computing: the storage devices themselves can become hardware-based roots of trust. Self-encrypting hard drives for laptop and desktop PCs have already emerged from leading vendors, and more are coming. Leading back-end storage solution providers have announced their intent to include incorporate hardware-based encryption in their disk storage offerings, with corresponding support from centralized key management software.

"The encrypting hard drive capabilities are helping us cross the river," said one enthusiastic proponent of trusted computing. "The acquisition of the self-encrypting drive as part of the standard PC procurement, and the subsequent ease of turning it on, is really helping to light up TPMs all around the enterprise."

User authentication. Leveraging the TPM to authenticate users is low-hanging fruit, whether as part of the pre-boot sequence, at Windows log-on, or for subsequent network and application access. About 40% of current TPM users in this study were using fingerprint biometrics or smart cards in conjunction with TPM for user authentication. We should also expect to see TPM support from leading One-Time Password (OTP) vendors in the future.

For certificate-based solutions, many of the same issues that challenged client-side PKI a few years ago need to be addressed for TPM-based deployments, such as lifecycle management for digital certificates and keys; centralized management infrastructure; and disaster recovery capabilities. Organizations evaluating TPM-based deployments should seek out vendors with proven solutions to address these issues.

Overall, organizations should ask their vendors for education and documentation about their support for trusted computing, both currently and on future product roadmaps. Some have existing capabilities but don't promote or document how to use it – an unnecessary missed opportunity to enhance enterprise security.

© 2008 Aberdeen Group.

Aberdeen Group
A Harte-Hanks Company

Chapter Three: Recommended Actions

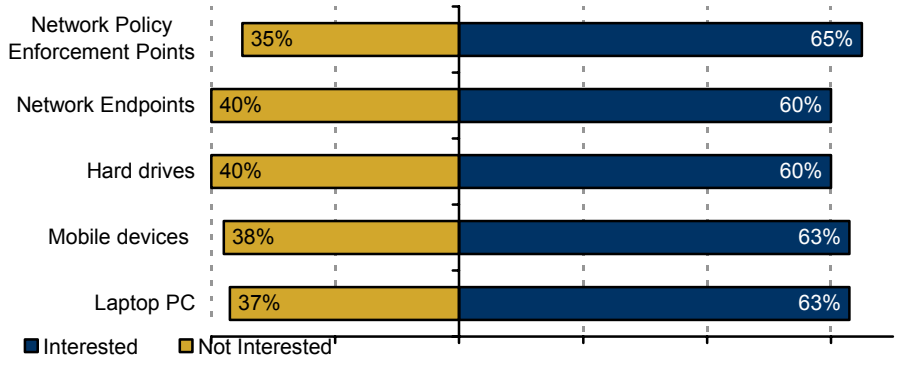
Whether a company is trying to move its performance in trusted computing from Laggard to Industry Average, or Industry Average to Best-in-Class, the following actions will help drive the necessary performance improvements:

General Recommendations for Trusted Computing

- Ask your existing vendors for detailed information about their support for trusted computing, both currently and in their future product roadmaps. Many of them have existing capabilities but may not have educated their sales teams or documented how to turn it on. All of them have product managers who are looking to their installed base to help them determine requirements for the next release.
- Specify support for trusted computing in your future procurement processes. Educate not only your IT staff, but also purchasing staff, on the opportunities to enable trusted computing. Staff members who are making the purchasing decisions may be thinking of the laptop as a commodity component, and need to think of it in connection to the organization's strategic security architecture. Include TPM requirements in all RFI and RFP specifications.
- If you haven't already deployed one or more applications based on trusted computing, launch a trusted computing pilot. Based on the research, the best immediate application opportunities are network access, data protection, and user authentication.

Across all respondents, research indicates a definite interest in learning more about trusted computing, with the strongest areas of interest shown in Figure 8.

Figure 8: Interest in TPM by Application Area



Source: Aberdeen Group, February 2008

Fast Facts

Across all respondents, over the last 12 months:

- √ 62% have increased the number of network users
- √ 79% have increased the number of remote users
- √ 61% have increased the number of wireless users
- √ 37% have increased the number of guest (non-permanent) users
- √ 71% have increased the total number of devices on the network

"Vendors like to elaborate on the umpteen different ways their solution can be operated, and meanwhile the poor schmucks who have to implement it are left wondering 'what part of that actually applies to me?'"

~ IT Director, Fortune 50 Enterprise

© 2008 Aberdeen Group.

Laggard Steps to Success

- Establish consistent policies for security and compliance. Less than half (48%) of Laggards reported current capabilities in this area. If we don't know where we are going, any road will take us there. After deciding clearly what should be done, communicate clearly with all affected employees regarding why it should be done and how to do it.
- Map risks and controls to the various regulations, standards, policies and best practices to which they relate. Just 40% of Laggards indicated this as a current capability, which is not surprising given the complex and changing nature of this task. Many companies start with a time-tested framework such as ISO 17799 / 27002 and build from there. For those who prefer to jumpstart their efforts with advice from an expert, countless vendors and service providers are available to help.
- Develop systematic processes for implementation and rollout of security solutions. Only 38% of Laggards reported this capability. Improvements should follow in the form of reduced human error and reduced ongoing management costs.

Industry Average Steps to Success

- Map risks and controls to the various regulations, standards, policies, and best practices to which they relate. At 44%, the Industry Average were only slightly better than Laggards in this regard. Consider starting with ISO 17799 / 27002 or another proven framework, or enlist the advice of a qualified third-party.
- Develop systematic processes for implementation and rollout of security solutions. Only half (50%) of the Industry Average reported this capability, compared to 68% of the Best-in-Class. Further, a net 31% of the Industry Average reported that deployment costs increased in the last 12 months (with none reporting a decrease), underscoring the direct financial impact of this process capability.

Best-in-Class Steps to Success

- Map risks and controls to the various regulations, standards, policies, and best practices to which they relate. Less than two-thirds (63%) of the Best-in-Class reported this capability. Consider starting with ISO 17799 / 27002 or another proven framework, or enlist the advice of a qualified third-party.
- Prioritize objectives for security controls as a function of risk, audit, and compliance requirements. About two-thirds (63%) of the Best-in-Class indicated this as a current capability. As described in previous research, improvements in this area will contribute to more effective allocation of IT resources as part of an overall security governance, risk management and compliance program.

© 2008 Aberdeen Group.

Aberdeen Group
A Harte-Hanks Company

Aberdeen Insights — Summary

Discussions about trusted computing often get bogged down in technical details such as what a TPM is, what functions it can perform, how its operation relates to network access control, encryption, user authentication, and so on. The current research, however, speaks directly to the business benefits of the trusted computing model. Analysis of current TPM users reveals that they have actually developed superior capabilities in the context of their overall security GRC programs. In other words, the data shows that top performance in trusted computing highly correlates with better security, sustained compliance, reduced human error, and lower cost of ongoing management.

Organizations wishing to improve their own performance in security governance, risk management and compliance should tune in to the benefits of trusted computing: educate within your company, engage with your strategic vendors, and make sure your organization is cognizant of both present and future opportunities to leverage trusted computing infrastructure.

And when the opportunity to leverage trusted computing infrastructure presents itself, turn it on. Like the seatbelt in your car or the treadmill in your basement, trusted computing infrastructure is beneficial only when it is actually used. Organizations should select the most immediate opportunity to pilot a trusted computing project to gain experience in the practical use and management of these solutions.

Send to a Friend

© 2008 Aberdeen Group.

Telephone: 617 723 7890
Fax: 617 723 7897

Aberdeen Group
A Harte-Hanks Company

Appendix A: Research Methodology

In January and February 2008, Aberdeen examined the range of approaches currently being taken in the deployment of applications based on the principles of trusted computing. The experiences and intentions of over 100 organizations from a diverse set of industries are represented in this study. Aberdeen supplemented this online survey effort with interviews with select survey respondents, gathering additional information on trusted computing strategies, experiences, and results.

Responding organizations had the following demographics:

- *Job title / function:* The research sample included respondents with the following job titles: C-level (32%); Vice President (4%); Director (11%); Manager (23%); Staff / Consultant (26%); and Other (4%). The largest segment by functional responsibility was IT, representing 57% of the sample.
- *Industry:* The research sample included respondents from a wide range of industries. The largest segments were Government / Aerospace / Defense (13%), Financial Services (15%), and High Tech (20%).
- *Geography:* The majority of respondents (67%) were from North America. Remaining respondents were from the Asia-Pacific region (15%) and Europe / Middle East / Africa (18%).
- *Company size:* Thirty-two percent (32%) of respondents were from large enterprises (annual revenues above US $1 billion); 32% were from midsize enterprises (annual revenues between $50 million and $1 billion); and 36% of respondents were from small businesses (annual revenues of $50 million or less).

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

© 2008 Aberdeen Group.

Aberdeen Group
A Harte-Hanks Company

Table 4: 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 2008

Table 5: 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 2008

Table 6: 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 2008

© 2008 Aberdeen Group.

Aberdeen Group
A Harte-Hanks Company

Appendix B:
Related Aberdeen Research

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

- Trusted Computing and Network Access; February 2008
- Trusted Computing and Data Protection; February 2008
- Trusted Computing and User Authentication; February 2008
- *Automating Encryption Key Management*; January 2008
- *Protecting Data at the Endpoints*; December 2007
- *Security Governance and Risk Management*; November 2007
- *Who's Got the NAC? Best Practices in Protecting Network Access*; October 2007
- *Sustaining Compliance*; September 2007
- *Encryption and Key Management*; August 2007

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

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

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

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

This document is the result of primary research performed by Aberdeen Group. Aberdeen Group's methodologies provide for objective fact-based research and represent the best analysis available at the time of publication. Unless otherwise noted, the entire contents of this publication are copyrighted by Aberdeen Group, Inc. and may not be reproduced, distributed, archived, or transmitted in any form or by any means without prior written consent by Aberdeen Group, Inc. 010908a