Aberdeen Group
A Harte-Hanks Company

Send to a Friend

Logical / Physical Security Convergence

Is it in the Cards?

December 2007

Aberdeen Group
A Harte-Hanks Company

Executive Summary

This research benchmark provides insight and recommendations for all organizations that are looking to integrate their logical security infrastructure and physical infrastructure as a component of taking a more strategic, enterprise-wide view of security risk. Data gathered for this report shows that companies with top performance in logical / physical security convergence have gained the business benefits of better physical security, better logical security, sustained compliance, faster response times, lower total cost, and improved collaboration between their logical and physical security teams.

Best-in-Class Performance

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

- Number of physical security-related incidents in the last 12 months
- Number of IT security-related incidents in the last 12 months
- Number of non-compliance incidents (e.g., failed audits) in 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 shared several common characteristics, including:

- 73% have conducted formal risk assessments
- 81% have prioritized logical security control objectives as a function of risk, audit, and compliance requirements
- 65% have prioritized physical security control objectives as a function of risk, audit, and compliance requirements
- 45% have implemented consistent security and compliance policies across both logical and physical security
- 55% have a clear mapping of risks and security controls to the various regulations, standards, policies, and best practices to which they relate
- 64% have implemented controls to monitor and verify that requirements of internal policies and external regulations are being satisfied

Recommended Actions

In addition to the specific recommendations in Chapter Three of this report, to achieve Best-in-Class results companies should give higher priority to logical / physical security convergence projects as a natural extension of taking a strategic, enterprise-wide view of security risk.

Research Benchmark

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

"The last thing anyone wants to do is create *new* silos to manage risk. Line of business managers are worried about meeting their MBOs, and they are tired of being peppered with one-off requests for security and compliance investments. What's more, they only know what they know within their own silo. Eventually this has to drive towards more integration, and towards common security governance and risk management at the C-level."

~ CIO, Insurance Company

Aberdeen Group
A Harte-Hanks Company

Table of Contents

Figures

Tables

Aberdeen Group
A Harte-Hanks Company

Chapter One: Benchmarking the Best-in-Class

Business Context

Several market drivers are combining to cause significant instances of integration (or "convergence") between logical security systems and physical security systems to take root:

- Based on the Homeland Security Presidential Directive 12 ("HSPD-12"), US federal agencies must issue a standards-compliant Personal Identity Verification (PIV) card to all employees and contractors by October 27, 2008. Such cards are expected to expand to additional large user communities (e.g., transportation workers and first responders) as well.
- In addition, although not directly driven by HSPD-12 compliance, many commercial organizations worldwide are also deploying solutions that integrate logical and physical access management on a standardized, card-based credential.
- In the back-end, emerging examples of convergence are motivated by improvements in visibility and risk management through centralized collection, normalization, and correlation of both logical and physical security information and events. Security Information and Event Management (SIEM) solutions, and to some extent Enterprise Single Sign-On (E-SSO) solutions, are discovering new use cases in logical / physical security convergence.
- Convergence examples are also being driven by new classes of network-enabled physical security solutions in areas such as building access, building automation, video surveillance and video analytics, and supervisory control and data acquisition systems.

Policy, planning, process, and organizational politics all play a role in the successful integration of logical security and physical security for any of the above examples. Recent Aberdeen research on *Security Governance and Risk Management* (November 2007) showed that by taking a more holistic view of risk, Best-in-Class organizations have demonstrated their ability to improve security, sustain compliance, improve leverage from existing IT resources, make faster decisions, optimize business processes, and improve visibility across organizational and geographical "silos."

Similarly, the current study reveals that Best-in-Class companies are nearly two-times more likely than Laggard organizations to view the convergence of logical and physical security as an integral part of their overall security governance and risk management strategy. For Industry Average companies, the tactical implementation and management of logical and physical security controls where specific needs exist is the most common approach (Figure 1).

Fast Facts

Best-in-Class strategies for logical / physical security convergence:

√ 76% develop a holistic view of security risks across the organization

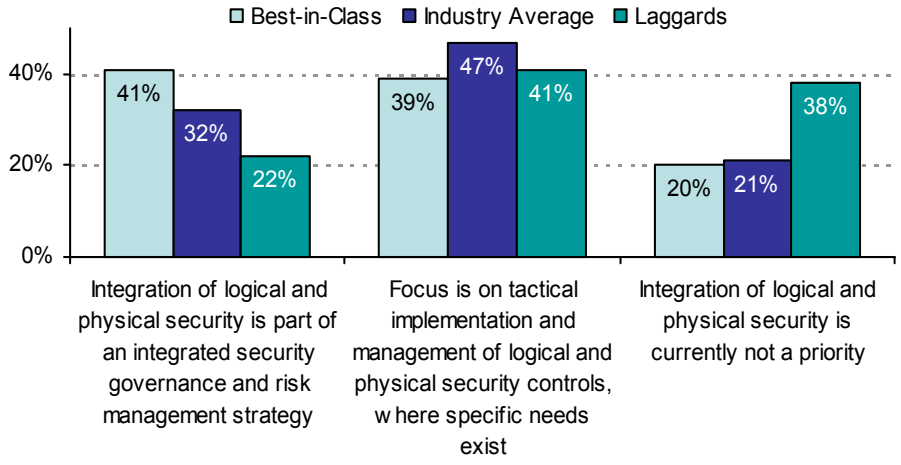
√ 65% establish and enforce consistent policies and procedures for both logical and physical security

"CEOs and boards don't really think about security; they think about risk. With too many security discussions, they kind of glaze over. But when you're talking with executive management and explaining things to them in terms of risk to the business, that really gets the business leaders thinking about integration and convergence of physical security and IT security in the right way."

~ Practice Leader, Global IT Services Provider

Aberdeen Group
A Harte-Hanks Company

Figure 1: Current Priority Given to Logical / Physical Security Convergence



Source: Aberdeen Group, December 2007

"It's not discrete just because it's traditionally been classified as logical security or physical security. Risk is risk."

~ CISO, Mid-Size Manufacturing Company

Most importantly, the research indicates that initiatives in integrating logical security and physical security are already helping Best-in-Class organizations to achieve superior performance in several critical areas:

- **Better physical security.** Compared to one year ago, a net **83%** of all Best-in-Class organizations **reduced the number of actual physical security incidents**; **40% reduced the average time to address** these incidents; and **27% reduced the total cost to address** them. In contrast, the Industry Average experienced more incidents than they did a year ago, took slightly less time to address them, and slightly **increased** their total cost to address them. The net performance of Laggards was worse compared to that of a year ago on all three measures.
- **Better logical security.** Compared to one year ago, a net **48%** of all Best-in-Class organizations **reduced the number of actual logical security incidents**; **31% reduced the average time to address** these incidents; and **22% reduced the total cost to address** them. In contrast, the Industry Average experienced more incidents than they did a year ago, took about the same time to address them, and slightly **increased** their total cost to address them. The net performance of Laggards was again worse compared to that of a year ago on all three measures.
- **Sustained compliance.** Compared to a year ago, a net **55%** of all Best-in-Class organizations **reduced the number of actual non-compliance incidents (e.g., failed audits)**; **59% reduced the average time to address** these incidents; and **35% reduced the total cost to address** them. In contrast, the Industry Average experienced roughly the same number of incidents as one year ago, took roughly the same time to address them, and a net 9%

increased their total cost to address them. The performance of Laggards was worse compared to that of a year ago on all three measures.

- **Better collaboration.** Compared to a year ago, a net **57%** of all Best-in-Class organizations **improved communication between their respective logical security and physical security teams**; **36% improved the coordination of responses** to security breaches by their logical security and physical security teams. This compares to 45% and 28%, respectively, for all respondents. More striking, Best-in-Class organizations were 16-times more likely than all respondents to have reduced the amount of human error related to logical and physical security, and nearly five-times more likely to have reduced the number of organizational and geographical "silos" for logical and physical security.

Compliance, taken in all of its dimensions – including compliance with government regulations, industry standards and best practices, industry regulations, and internal policies – is a leading driver for current investments in logical / physical security convergence, consistent with previous Aberdeen research on other IT security initiatives. Across all respondents, protecting the organization and its brand also continues to surface as a leading driver. Best-in-Class organizations also identified reducing the costs of implementing and managing security controls as a driver of their current investments in logical / physical security convergence.

On the other side of the coin, the most commonly cited reasons that organizations had *not* invested in logical / physical security convergence initiatives include: 49% of organizations indicated that other projects are perceived as higher priority, and 37% indicated that the costs are perceived as too high. In light of the aforementioned business benefits, however, companies would do well to give logical / physical security convergence opportunities a closer look.

Aberdeen's Maturity Class Framework

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

- Number of physical security-related incidents in the last 12 months
- Number of IT security-related incidents in the last 12 months
- Number of non-compliance incidents (e.g., failed audits) in the last 12 months

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.)

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	▪ 83% **decreased** the number of physical security-related incidents in the last 12 months ▪ 48% **decreased** the number IT security-related incidents in the last 12 months ▪ 55% **decreased** the number of non-compliance incidents (e.g., failed audits) in the last 12 months
Industry Average: Middle 50% of aggregate performance scorers	▪ 12% **increased** the number of physical security-related incidents in the last 12 months ▪ 5% **increased** the number IT security-related incidents in the last 12 months ▪ 4% **decreased** the number of non-compliance incidents (e.g., failed audits) in the last 12 months
Laggard: Bottom 30% of aggregate performance scorers	▪ 45% **increased** the number of physical security-related incidents in the last 12 months ▪ 41% **increased** the number IT security-related incidents in the last 12 months ▪ 32% **increased** the number of non-compliance incidents (e.g., failed audits) in the last 12 months

Source: Aberdeen Group, December 2007

The Best-in-Class PACE Model

Achieving superior results in integrating logical security and physical 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 Framework, see Table 4 in Appendix A). The characteristics exhibited by Best-in-Class organizations in this benchmark study are summarized in Table 2.

Table 2: The Best-in-Class PACE Framework for Logical / Physical Security Convergence

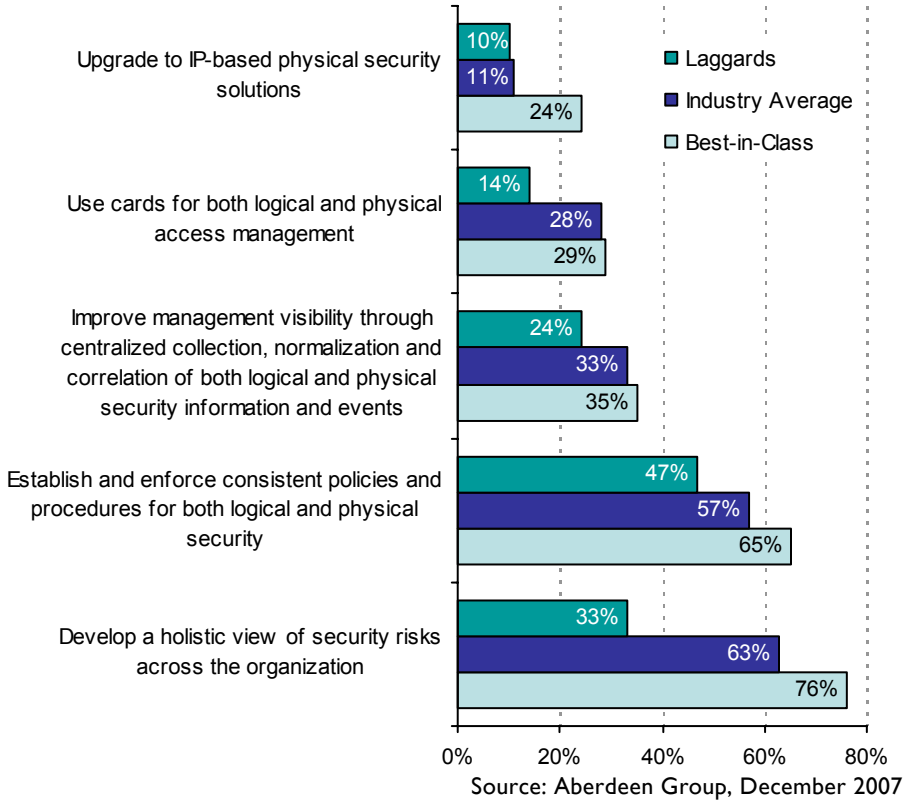
Pressures	Actions	Capabilities	Enablers
▪ Protect the organization and its brand ▪ Government regulations ▪ Industry best practices and standards ▪ Risks associated with information assets	▪ Develop a holistic view of security risks across the organization ▪ Establish and enforce consistent policies and procedures for both logical and physical security ▪ Improve management visibility through centralized collection, normalization, and correlation of both logical and physical security information and events ▪ Use cards for both logical and physical access management	▪ Formal risk assessments ▪ Both logical security and physical security control objectives are prioritized as a function of risk, audit, and compliance requirements ▪ Consistent security and compliance policies across both logical and physical security ▪ Responsible executive or team with primary ownership for security risk, including both logical and physical security ▪ Formal documentation, awareness, and end-user training programs around both logical security and physical security ▪ Formal communication channels between logical and physical security teams ▪ Collaborative planning between logical and physical staff regarding security policies ▪ Clear mapping of risks and controls to the various regulations, standards, policies, and best practices to which they relate ▪ Consistent, unified view of logical and physical security risks (elimination of silos of information and analysis) ▪ Controls to monitor and verify that requirements of internal policies and external regulations are being satisfied	▪ Vulnerability management ▪ Configuration and change management ▪ Patch management ▪ Network Access Control (NAC) ▪ Log management ▪ Security Information / Event Management (SIEM) ▪ Identity and Access Management (IAM) ▪ Public-Key Infrastructure (PKI) ▪ Smart cards and card management systems ▪ Biometrics (fingerprint) ▪ Photo ID cards ▪ Building access cards and Physical Access Control Systems (PACS) ▪ RFID-enabled building access cards ▪ Video surveillance (network-based)

Source: Aberdeen Group, December 2007

Best-in-Class Strategies

Figure 2 illustrates the strategic actions identified in our research that are driving current investments in logical / physical security convergence initiatives. More than three-fourths (76%) of Best-in-Class companies in the current survey develop a holistic view of security risks across the organization – breaking the traditional "siloed" approach of separate logical security and physical security perspectives. In contrast, 63% of the Industry Average and only 33% of Laggards indicated this enterprise-wide approach. Nearly two-thirds (65%) of the Best-in-Class establish and enforce consistent policies and procedures for both logical and physical security, compared to 57% of the Industry Average and 47% of Laggards.

Figure 2: Strategic Actions Driving Current Investments in Logical / Physical Security Convergence Initiatives



Source: Aberdeen Group, December 2007

In addition, with respect to current investments involving integration of logical security systems and physical security systems, the research also indicates three distinct use cases that differentiate the Best-in-Class organizations from other survey respondents (Figure 2):

- **Security information and events.** By collecting and correlating information and events from both logical security and physical security infrastructures, companies can improve overall management visibility and establish an enterprise-wide view of risk. While this capability is just now emerging, the Best-in-Class in the current study are currently 1.5-times more likely than Laggards to be investing in this approach.
- **Cards.** The use of cards (as the common basis for both logical and physical access management) is a well-known example of logical / physical security convergence. Driven by compliance with HSPD-12 in the US Federal government, card-based convergence is also beginning to take root in many large commercial enterprises. In the current study, the Best-in-Class are currently two-times more likely than Laggards to be investing in integration of logical security and physical security based on common access cards.

- **IP-based physical security.** As new classes of IP-enabled physical security solutions are rolled out – in areas such as building access, building automation, video surveillance and video analytics, and supervisory control and data acquisition systems – additional logical / physical security convergence opportunities are beginning to emerge. Best-in-Class organizations in the current study are currently nearly 2.5-times more likely than Laggards to be investing in this approach by upgrading to physical security solutions based on standard IP-based networks.

As noted, Best-in-Class organizations are employing strategies to develop an enterprise-wide view of risk, and to establish consistent security policies. In doing so, they are gaining the business benefits of better physical security, better logical security, sustained compliance, faster response times, lower cost, and improved collaboration between logical and physical security teams. In the next chapter, we describe what the top performers are doing to achieve these gains.

Aberdeen Insights - Strategy

Previous Aberdeen research showed that through their emerging capabilities in the area of security governance and risk management, Best-in-Class companies are taking proactive steps to ensure that their investments in security and compliance controls directly support their objectives for the business. A consistent, enterprise-wide view of security risk – integrating both physical security and IT security – is a sensible element of this strategy. By combining superior security governance and risk management with an integrated approach to logical and physical security, Best-in-Class organizations set themselves up to compete in the global economy with a distinct advantage: not only with an optimized IT infrastructure, but also with better protection for their digital, physical, and human assets.

Logical / physical security convergence opportunities are made possible by key enabling technologies (e.g., common access cards, security information and event management systems, enterprise single sign-on systems, and new classes of IP-based physical security systems), but policy, planning, process, and organizational politics each play a prominent role in successful implementations. Aberdeen's research indicates that inattention and inertia, rather than technology issues, may be the two biggest obstacles to the acceleration of logical / physical security integration in the near term.

Is logical / physical security convergence in the cards? Yes – literally in some cases, but more generally as a natural extension of taking a strategic, holistic view of security risk. Convergence projects will be fueled by the demonstrable business benefits of better security, sustained compliance, faster response times, lower costs, and improved collaboration.

"We have multiple teams, working on multiple projects, probably wasting a lot of dollars in overlap and duplication. Most of them will say 'I'm too busy to work on integration; I'm working on…' whatever is the flavor of the day. Our IT security and physical security teams share a common purpose - to protect the company - but other than that, they currently have nothing else in common."

~ Business Unit Manager, US Manufacturing Company

Aberdeen Group
A Harte-Hanks Company

Chapter Two: Benchmarking Requirements for Success

The selection of specific logical / physical security integration opportunities, 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, lower cost, and improved collaboration.

Case Study - Microsoft, Redmond, WA

Microsoft, with revenues of more than $51B in the fiscal year ending June 30, 2007 and approximately 79,000 full-time employees worldwide, is one of the best known non-government examples of full-scale commitment to integration of logical security and physical security based on multi-purpose smart cards.

Because it stores and processes significant amounts of personally identifiable information, Microsoft pays close attention to security controls (both logical and physical) that protect its sensitive data. The improper disclosure of such information could harm its reputation and subject the company to liability under laws that protect personal data, resulting in increased costs or loss of revenue. As part of its response, Microsoft trains both employees and vendors on data security, and implements many other best practices to protect its valuable information assets. Eliminating the dependence on simple username / password for user authentication, by issuing smart cards for every employee, was a highly visible element initiated more than three years ago.

"The move we made to smart cards was initially driven from a security perspective, not an operational-cost perspective," said a Microsoft spokesperson. "Enterprises are increasingly willing to make the investment to solve these kinds of problems."

What arguably began as purely an additional cost, however, has evolved to a converged capability that both cuts costs and enhances security and compliance. In addition, Microsoft's internal use of its own digital certificate-based technologies helps to accelerate logical / physical convergence capabilities in the general market. Today, Microsoft's corporate-wide commitment to card-based identities has evolved to multi-purpose smart cards with applications that include:

- Entry into Microsoft buildings through integration with their physical access-control system
- Smart-card authentication to the desktop
- Authentication for network access
- Authentication for Intranet access, to hundreds of sites worldwide
- Authentication for remote access, including support for thousands of telecommuters
- Privileged access to servers (e.g., for administrative purposes)
- Signing and encrypting e-mail

Fast Facts

Compared to all respondents, Best-in-Class organizations are:

√ **Five-times** more likely to have reduced the time required to issue card-based credentials to a new employee (issuance / provisioning)

√ **Three-times** more likely to have reduced the time to revoke card-based credentials for a terminated employee, and to revoke access to the resources to which that employee had access (revocation / de-provisioning)

√ **Two-times** more likely to have increased the overall convenience to end-users of card-based solutions

Competitive Assessment

The aggregated performance of surveyed companies determined whether they ranked as Best-in-Class, Industry Average, or Laggard. In addition to having common performance levels, each class also shared characteristics in five key categories: (1) **Process** (the ability to detect and respond to changing conditions without placing additional burdens on the organization); (2) **Organization** (corporate focus and collaboration among stakeholders); (3) **Knowledge Management** (contextualizing data and exposing it to key stakeholders); (4) **Technology** (the selection of appropriate tools, and the intelligent deployment of those tools); and (5) **Performance Management** (the ability of the organization to measure the benefits of technology deployment and use the results to further improve key processes). These characteristics (identified in Table 3) serve as a guideline for best practices, and correlate directly with Best-in-Class performance across the key metrics.

Table 3: Competitive Framework

	Best-in-Class	Average	Laggards
Process	Formal risk assessments		
	73%	55%	52%
	Logical security control objectives prioritized as a function of risk, audit, and compliance requirements		
	81%	45%	42%
	Physical security control objectives prioritized as a function of risk, audit, and compliance requirements		
	65%	53%	39%
	Consistent security and compliance policies across both logical and physical security		
	45%	29%	24%
	Combined collection, normalization, and correlation of both logical and physical security information and events		
	19%	16%	12%
Organization	Responsible executive (or team) with primary ownership for security risk, including both logical and physical security		
	57%	54%	50%
	Formal documentation, awareness, and end-user training programs around logical security		
	55%	45%	42%
	Formal documentation, awareness, and end-user training programs around physical security		
	50%	48%	45%
	Formal employee / contractor job definitions and logical / physical access policies		
	73%	55%	28%
	Collaborative planning between logical and physical staff regarding security policies		
	36%	26%	24%
	Cross-training between logical and physical security teams		
	23%	16%	12%

	Best-in-Class	Average	Laggards
Knowledge	Clear mapping of risks and controls to the various regulations, standards, policies, and best practices to which they relate		
	55%	26%	18%
	Consistent, unified view of logical and physical security risks (elimination of silos of information and analysis)		
	29%	18%	16%
Technology	Controls to monitor and verify that requirements of internal policies and external regulations are being satisfied		
	64%	45%	36%
	Logical / physical security technologies currently in use		
	See Figure 3 and Figure 4		
Performance	Identification of all information required for auditing and reporting		
	71%	49%	27%
	Identification of required frequency for auditing and reporting		
	52%	38%	24%

Source: Aberdeen Group, December 2007

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 created competitive advantage through logical / physical security integration.

Process

Best-in-Class organizations surveyed are generally more disciplined about the process of security governance and managing risk across both IT security and physical security domains. Most (73%) conduct formal risk assessments, and 81% prioritize their logical security control objectives as a function of risk, audit, and compliance requirements – nearly two-times the rate of the Industry Average and Laggard organizations. On the physical security side of the house, the Best-in-Class were slightly less disciplined (65% prioritized their physical security control objectives as a function of risk, audit, and compliance requirements), and the gap with the Industry Average and Laggards was slightly less. Under half (45%) of the Best-in-Class indicated that they currently have consistent security and compliance policies across both logical and physical security, though this was 1.5-times higher than the Industry Average. The positive trend is towards bringing the logical security and physical security management processes more in alignment.

Aberdeen Group
A Harte-Hanks Company

Organization

In much of Aberdeen's research on IT security topics, the use of particular enabling technologies and optimization of business processes tend to dominate the differentiation between the Best-in-Class organizations and other respondents. In the case of logical / physical security convergence, however, the organizational aspects and collaboration among stakeholders play a major role.

The three maturity classes are reasonably close to one another with respect to formal documentation, awareness, and end-user training programs around both logical and physical security. A much larger difference is evident regarding the presence of formal job definitions for employees and contractors, and the associated logical and physical access policies – 73% of the Best-in-Class currently have these, a factor of 2.6-times higher than Laggards.

The focus on organizational aspects is not only on communicating to the end-users, however, but also on communicating between the IT security and physical security teams themselves. Only a third (36%) of the Best-in-Class currently do collaborative planning between logical and physical security staff regarding security policies, and less than a fourth (23%) currently conduct cross-training between their logical and physical security teams. Taking deliberate steps to build bridges between these organizations (independent of the reporting structure) is a critical element of any logical / physical security convergence initiative.

Knowledge Management

The first aspect of knowledge management – putting data in context – is a significant differentiator for Best-in-Class organizations in our study. More than half (55%) have made a clear mapping of risks and controls to the various regulations, standards, policies, and best practices to which they relate. This is three-times the rate by Laggard organizations, although even the Best-in-Class have a great deal of opportunity for improvement in this area.

The second aspect of knowledge management – exposing data in context to the key stakeholders – is a major opportunity for improvement across the board. Although the Best-in-Class are nearly two-times more likely to have eliminated silos of information and analysis by providing a consistent, unified view of logical security and physical security risks, at 29% even the Best-in-Class can make great strides in this regard.

Technology

The research illustrated multiple examples of logical / physical security convergence, based on a variety of enabling technologies (Figure 3 and Figure 4). In the case of card-based solutions, 32% of all respondents in the current survey had currently deployed smart cards and card management systems, with another 25% planning deployment in the next 12 months (78% year-over-year growth). Public-Key Infrastructure (PKI) and digital

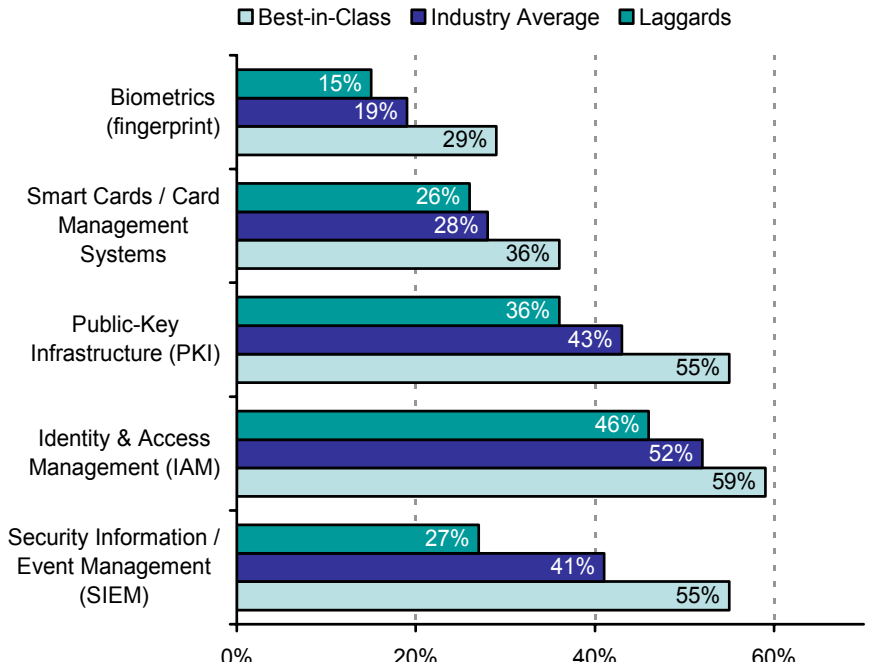
Telephone: 617 723 7890
Fax: 617 723 7897

certificates was already in place at 43% of all respondents, with another 12% planning deployment in the next year (28% year-over-year growth).

Fingerprint biometrics – often deployed in conjunction with smart cards – were currently in use by 24% of all respondents, with another 13% planning deployment in the next 12 months (54% year-over-year growth). Notably, the Best-in-Class organizations in the study were two-times more likely than Laggards to deploy fingerprint biometrics.

Back-end integration of security information and events, enabled by SIEM systems, was currently deployed by 55% of Best-in-Class organizations in the study – fully two-times the rate of Laggards. In addition to the existing set of SIEM vendors coming from the IT security segment, new SIEM-like solutions are also beginning to emerge from the physical security market. The positive news behind this trend is evidence for increasing logical / physical security convergence in the context of managing enterprise-wide risk. The potential downside is the unnecessary confusion that may ensue as vendors (and many analysts) invent new categories in an effort to differentiate themselves.

Figure 3: Selected Logical Security Technologies Currently in Use



Source: Aberdeen Group, December 2007

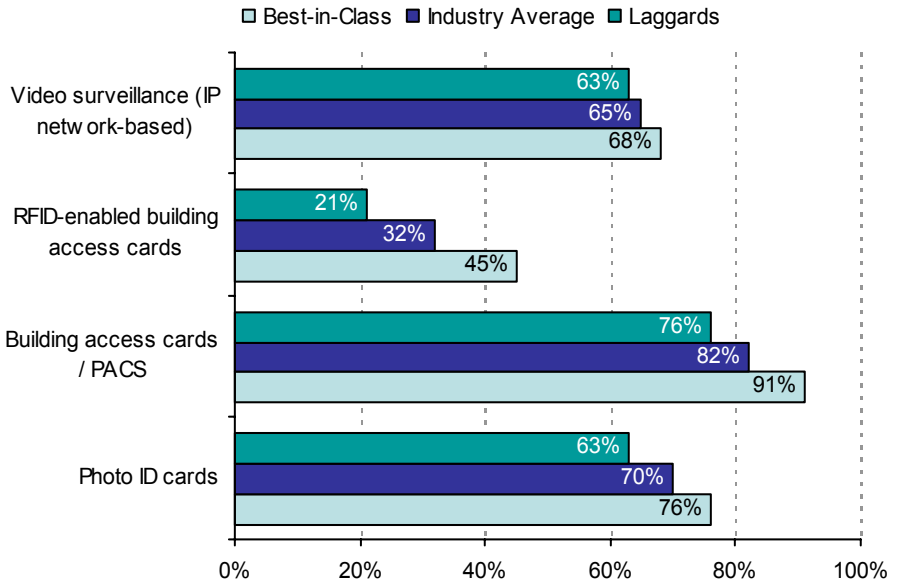
"Everybody is climbing the mountain just to issue the cards - but once they get to the top, they discover that these cards cannot really be used for much of anything. Like everything else, the real integration - on the application side - will probably take place over the next two or three years. But the fact that the cards have been issued is actually a huge catalyst to leverage these investments, which will in time create significant business value."

~ Program Manager
US Systems Integrator

In the domain of physical security, the research indicates that building access cards and Physical Access Control Systems (PACS) are already widely deployed (82% of all respondents). Proximity-based building access cards, however, were currently deployed by only 31% of all respondents, with another 14% indicating plans to deploy in the next year (45% year-over-year growth).

Finally, IP-based video surveillance technologies are currently deployed by about two-thirds of all respondents, which has created a growth opportunity for providers of video analytics solutions – basically, there are not enough eyeballs to monitor and analyze the volume of video data that is being captured, and video analytics software provides the intelligence to analyze video for specific objects, data, and behavior. Video analytics solutions are currently deployed by 15% of all respondents in this study, with another 18% indicating planned deployment in the next 12 months (120% year-over year growth).

Figure 4: Selected Physical Security Technologies Currently in Use



Source: Aberdeen Group, December 2007

Performance Management

The Best-in-Class organizations in our survey were substantially better than their counterparts in identifying all information required for auditing and reporting (71%, 2.6-times better than Laggards) and the required frequency for auditing and reporting (52%, 2.2-times better than Laggards). Knowing what and how frequently information is needed when integrating IT security and physical security controls is a key success factor for moving towards a consistent, enterprise-wide view of security risk.

Aberdeen Group
A Harte-Hanks Company

Aberdeen Insights - Technology

The problem with logical / physical security convergence opportunities is that there are so many from which to choose.

Using a single device (smart card, or other token) is one common starting point, a positive step towards the greater vision of IT access, building access, photo ID, and even inter-organizational trust housed within a single converged "container". But issuing devices is merely the tip of the iceberg. Even though both logical credentials and physical credentials may be tied to the same physical device, logical identities and physical identities must also be correlated at the management level. In most organizations, card lifecycle management processes and physical access control management processes remain separate – not only technologically, but also organizationally – with duplication of business processes and increased total cost.

Given that Physical Access Control Systems (PACS) have extremely long replacement cycles (as one respondent pointed out, "there is no rip-and-replace for these systems"). The trend will be towards more cooperation and integration between card management systems, identity and access management systems, and PACS systems. Solution providers that can most effectively bridge the gaps in these technology areas will be best-positioned to drive new logical / physical convergence opportunities.

Another priority is to begin looking beyond mere issuance of cards or other tokens (e.g., to meet deadlines mandated by HSPD-12), to focus on how these credentials can be leveraged for multiple purposes. "Rather than just having it in the badge holder," as one manager from a government agency noted, "it's about the applications." Convergence initiatives are driving digital certificates towards their long-held promise as a common basis for identity across a broad range of applications.

Correlating information and events across both logical and physical domains, with common auditing and reporting, is another immediate opportunity for convergence identified in the research. SIEM solution providers, and to some extent E-SSO solution providers, have recently started to orient their solutions around logical / physical security convergence opportunities.

Finally, new examples of convergence are also being driven by new classes of network-enabled physical security solutions, in areas such as building access, building automation, video surveillance and video analytics, and supervisory control and data acquisition systems. These topics may be explored in more detail in future Aberdeen benchmark reports.

Aberdeen Group
A Harte-Hanks Company

Chapter Three: Recommended Actions

Whether a company is trying to move its performance in logical / physical security convergence 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

- **Map the compliance landscape.** Less than one in five (18%) Laggard organizations have established a clear mapping of risks and controls to the various regulations, standards, policies, and best practices to which they relate. Small wonder, as this is a complex and changing task. Many companies start with a proven framework (such as ISO 17799 / 27002) and build from there. Numerous vendors and service providers are available to help for those who prefer to jumpstart their efforts with advice from an expert.
- **Identify requirements for auditing and reporting.** About one in four Laggard organizations have identified all information required for auditing and reporting, and the required frequency of auditing and reporting (27% and 24%, respectively). A lyric from a Gladys Bentley song comes to mind: "Find out what they like, and how they like it, and give it to them just that way."
- **Prioritize both logical and physical security control objectives as a function of risk, audit, and compliance requirements.** Roughly four in 10 Laggard organizations surveyed have prioritized logical security control objectives and physical security control objectives as a function of risk, audit, and compliance requirements (42% and 39%, respectively). Keep in mind that a fundamental purpose for logical / physical security convergence initiatives is to establish consistent, enterprise-wide management of security risk.

Industry Average Steps to Success

- **Map the compliance landscape.** The Industry Average were slightly better than Laggards in mapping the compliance landscape - 26% of Industry Average organizations had clearly associated specific risks and controls to the various regulations, standards, and best practices to which they relate. Consider building on an industry standard framework such as ISO 17799 / 27002, or enlist the services and advice of a qualified expert.
- **Prioritize both logical and physical security control objectives as a function of risk, audit, and compliance requirements.** The Industry Average were slightly better (45%) than Laggard organizations at prioritizing logical security control

Fast Facts

Percentage of Best-in-Class organizations surveyed that issue and use cards:

- √ 95% for building access
- √ 74% for photo identification badges
- √ 32% for remote access (e.g., VPN)
- √ 32% for IT systems access

objectives as a function of risk, audit, and compliance requirements, and had a wider margin (54%) with respect to physical security control objectives. Improving both as part of logical / physical security convergence initiatives will advance the ball towards the goal of achieving a consistent, enterprise-wide view of security risk.

- **Establish consistent policies.** Only 29% of Industry Average organizations surveyed had established consistent security and compliance policies across both logical and physical security. Consistent policy will not only guide the selection of enabling technologies for specific logical / physical security convergence initiatives, but will also help to drive the expected business benefits of better physical security, better logical security, sustained compliance, faster response times, lower cost, and improved collaboration between logical and physical security teams.

"I simply made the IT security guys and the physical security guys sit down with each other. People tend to see things differently after they break bread together."

~ CEO, Publishing Company

Best-in-Class Steps to Success

- **Establish consistent policies.** Less than half (45%) of the Best-in-Class organizations surveyed have established consistent security and compliance policies across both logical and physical security. This represents a large opportunity for improvement, and will serve as a guideline for project selection, technology selection, measures and targets, and funding. The common purpose is to improve the protection of the company, including its digital assets, its physical assets, and its people.
- **Build bridges between organizations.** Nearly six out of 10 (57%) Best-in-Class companies surveyed had a responsible executive or team with primary ownership for security risk, including both logical and physical security. Steps should be taken to increase collaborative planning between logical and physical staff regarding security policies, something currently done by only 36% of the Best-in-Class. In addition, cross-training between logical and physical security teams, currently done by just 23% of the Best-in-Class, will improve communication and strengthen both organizations.
- **Eliminate silos of information.** Just 29% of the Best-in-Class indicated that they had eliminated silos of information and analysis through a consistent, unified view of logical and physical security risks. Only 19% currently collect, normalize, and correlate both logical and physical security information and events. Putting this data in context and exposing it to key stakeholders on both logical security and physical security teams will accelerate the realization of the material business benefits identified in this study.

"Nobody wants to get a thick report that basically tells them everything is okay. They just want to get immediate notice about exceptions, and the ability to drill down to determine their root cause."

~ IT Manager, Healthcare Industry

Aberdeen Group
A Harte-Hanks Company

Aberdeen Insights - Summary

By combining superior security governance and risk management with an integrated approach to logical and physical security, Best-in-Class organizations set themselves up to compete in the global economy with a distinct advantage: not only with an optimized IT infrastructure, but also with better protection for their digital, physical, and human assets.

Leaders with experience in successful logical / physical security convergence implementations say that the single most important thing a company can do is appoint a strong internal project manager. Assuming that the logical / physical security convergence initiative has a clear executive sponsor, key characteristics for this leadership position include:

- Experienced - knows the discipline of project management
- An employee of the company (not a consultant or vendor-appointed project manager)
- Respected throughout the organization
- Strong communication skills - able to bridge the gap between logical and physical teams
- Fair and impartial - ensures that all functions represented on the project team have equal input and authority

Although made possible by the ongoing evolution of technologies and standards, the real impetus for moving logical / physical security convergence projects to a higher priority should be the demonstrable business benefits identified in this study: better protection of digital assets, physical assets, and people; sustained compliance; faster response times; lower costs; and improved collaboration between teams.

Telephone: 617 723 7890
Fax: 617 723 7897

Aberdeen Group
A Harte-Hanks Company

Appendix A: Research Methodology

In December 2007, Aberdeen examined the range of approaches currently being taken to address the integration ("convergence") of logical security and physical security. The experiences and intentions of nearly 140 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 logical / physical security convergence 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 (30%); Vice President (7%); Director (21%); Manager (18%); Staff / Consultant (20%); and Other (4%).
- *Industry:* The research sample included respondents from a wide range of industries. Government / Aerospace / Defense represented 15% of the sample. Other notable segments include Financial Services (7%); Healthcare (6%); Education (6%); and High Tech (27%).
- *Geography:* The majority of respondents (75%) were from North America. Remaining respondents were from Europe, Middle East and Africa (17%) and the Asia-Pacific region (8%).
- *Company size:* Twenty-two percent (22%) of respondents were from large enterprises (annual revenues above US $1 billion); 35% 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).

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

Study Focus

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

- √ The degree to which logical security and physical security controls are being integrated in the context of overall enterprise risk
- √ The structure and effectiveness of existing logical / physical convergence implementations
- √ Current and planned use of enabling technologies related to logical / physical security integration
- √ The benefits, if any, that have been derived from logical / physical security convergence initiatives

The study aimed to identify emerging best practices for logical / physical security convergence, and to provide a framework by which readers could assess their own capabilities and performance.

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, December 2007

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, December 2007

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 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 those decisions.

Source: Aberdeen Group, December 2007

Aberdeen Group
A Harte-Hanks Company

Appendix B:
Related Aberdeen Research

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

- *Security Governance and Risk Management;* November 2007
- *Sustaining Compliance* September 2007
- *Encryption and Key Management;* August 2007
- *Protecting Cardholder Data;* June 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