



Best Practices in Choosing and Consuming Managed Security Services

Google is happy to provide you with this Aberdeen Group research paper that will help you in evaluating how cloud computing security solutions can benefit your business.

As many of the Best-in-Class organizations featured in this report know, cloud computing offers effective solutions that improve security while reducing cost and the complexity of your IT infrastructure.

Google Message Security, powered by Postini, is a cloud computing solution that provides highly effective inbound and outbound email security for organizations of all sizes. It simplifies the task of managing security and compliance of email messages and frees up valuable IT resources.

For more information on Google Message Security and the full line of Google Apps solutions for businesses and organizations, please visit:
<http://www.google.com/a/security>



Your complimentary access to this Aberdeen Group report is made possible through a special distribution license granted to Google, Inc. Aberdeen Group bears sole responsibility for the research findings and analysis included in this report. The findings and views expressed in this report do not necessarily reflect the views of the licensee.

Best Practices in Choosing and Consuming Managed Security Services

January 2008



Executive Summary

The need for greater security is compelling organizations to consider using Managed Security Service Providers (MSSPs) for some or all of their IT security needs. Companies that are getting the best results from a security performance perspective all use managed security services as part of their IT security. This report looks at how these companies choose to acquire and consume managed security services, including ways mature MSSP customers have learned to get the best value from their MSSPs.

The potential benefits to organizations that consume security solutions as managed services are widespread. Organizations can improve their security and compliance performance, reduce the management overhead associated with managing security solutions themselves, avail themselves of security solutions that would otherwise be unaffordable, avail themselves of security protection "in the cloud" – thus, stopping threats such as denial of service attacks before they actually reach the organization. In addition, they can avail themselves of security expertise that is unavailable or unaffordable within their own organization.

Best-in-Class Performance

Aberdeen used four key performance criteria to distinguish Best-in-Class (BIC) companies:

- A significant decrease in help desk cost attributed to security
- A significant decrease in the number of security incidents
- The number of data loss incidents
- The number of malware infections

Competitive Maturity Assessment

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

- 86% report zero failed audits
- 64% have established Service Level Agreements (SLAs) with their MSSPs
- 63% use pre-emptive planning to address the most likely risk

Required Actions

In addition to the recommendations in Chapter Three of this report, to achieve Best-in-Class performance, companies must pro-actively manage their MSSPs. Companies should define processes and criteria for choosing and vetting potential MSSPs, establish metrics and SLAs to hold them accountable, and regularly re-evaluate and ensure that their choices are critical to ultimate success of the business.

Research Benchmark

Aberdeen's Research Benchmarks provide an in-depth and comprehensive look into process, procedure, methodologies, and technologies with best practice identification and actionable recommendations

"We are pretty happy with our current provider. But past experience has shown the importance of auditing the providers. So we are building out our own IDS and firewall monitoring solutions strictly as a backup and audit function."

~ IT and Network Security
Director, \$1.5B Sales and
Marketing Services Firm

Send to a Friend 

Table of Contents

Executive Summary.....	2
Best-in-Class Performance.....	2
Competitive Maturity Assessment.....	2
Required Actions.....	2
Chapter One: Benchmarking the Best-in-Class.....	4
The Need for Improved Security - Number One Driver.....	4
The Maturity Class Framework.....	5
The Best-in-Class PACE Model.....	6
Best-in-Class Strategies.....	7
Chapter Two: Benchmarking Requirements for Success.....	9
Competitive Assessment.....	10
Capabilities and Enablers.....	11
Chapter Three: Required Actions.....	14
Laggard Steps to Success.....	14
Industry Average Steps to Success.....	14
Best-in-Class Steps to Success.....	15
Appendix A: Research Methodology.....	16
Appendix B: Related Aberdeen Research.....	18

Figures

Figure 1: Best-in-Class Organizations Tell Why They Use Managed Security Services.....	4
Figure 2: Best-in-Class Strategies for Consuming Managed Security Services.....	7
Figure 3: Types of Service Level Agreements.....	12

Tables

Table 1: Top Performers Earn Best-in-Class Status.....	5
Table 2: The Best-in-Class PACE Framework.....	7
Table 3: The Competitive Framework.....	10
Table 4: The PACE Framework Key.....	17
Table 5: The Competitive Framework Key.....	17
Table 6: The Relationship Between PACE and the Competitive Framework.....	17

Chapter One: Benchmarking the Best-in-Class

The Need for Improved Security - Number One Driver

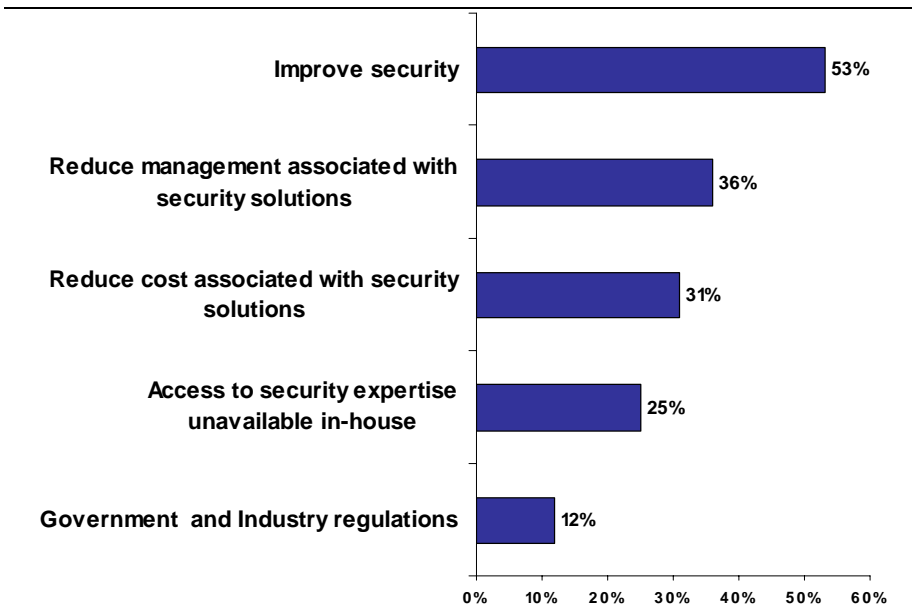
Managed security services of one kind or another have been available for more than 10 years. The delivery of all kinds of managed services has expanded and most security solutions are now being offered as a managed service.

The expanding threat landscape and vast spectrum of solutions needed to combat it is pushing organizations to recognize that they can get better security by putting at least some of their security into the hands of Managed Security Service Providers (MSSPs). In-depth interviews revealed that integral to their decision to use an MSSP is the lack of knowledgeable staff to manage the various aspects of their IT vulnerability. But beyond the lack of expertise, beyond the challenges of managing security solutions, even beyond potential cost savings, organizations have recognized that at least in some areas of security, they can actually get better protection by using a managed security service. To bring this point home, Aberdeen research reveals that across all respondents, improving security is the top driver for adopting managed security services; Best-in-Class organizations are nearly twice as likely to cite improving security as the Industry Average.

Fast Facts

- ✓ 100% of Best-in-Class organizations consume some managed security services as part of their security strategy
- ✓ 86% of Best-in-Class organizations report zero failed audits

Figure 1: Best-in-Class Organizations Tell Why They Use Managed Security Services



Source: Aberdeen Group, January 2008

The belief that managed security services can yield better results from a performance perspective is born out by results garnered by Best-in-Class companies.

Although not the strongest motivation in deciding to pursue managed security services, Best-in-Class companies have better results in reducing the number of failed audits and penalties resulting from failure to comply. Managed security services often play a key role in improving compliance by providing standardized, consistent documentation in terms of logs and reports, and by separating the auditing from the audited organization, creating a separation of duties and shielding organizations from complaints of compromised data.

Best-in-Class companies greatly reduced the incidence of sabotage. As organizations contend more with insider threats, having elements of the organizations security outside of the immediate access of direct employees can act as a deterrent to some malicious activities.

The Maturity Class Framework

Aberdeen used four key performance criteria to distinguish the Best-in-Class from Industry Average and Laggard organizations:

- Significant decrease in the number of security incidents
- Significant decrease in the cost of help desk support attributed to security incidents
- The actual number of malware infections
- The actual number of data loss incidents

The companies that achieved Best-in-Class performance had zero or minimal number of incidents of data loss and malware infections and significantly decreased the number of security incidents and the cost of help desk support attributable to security incidents. The Best-in-Class showed demonstrably better results in many other performance indicators as well.

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

Definition of Maturity Class	Mean Class Performance
<p>Best-in-Class: Top 20% of aggregate performance scorers</p>	<ul style="list-style-type: none"> ▪ 69% reduced the number of security incidents by more than 20% ▪ 45% decreased the cost of help desk support attributed to security incidents by more than 20% ▪ 92 % report 10 or fewer malware infections ▪ 72% report zero data loss incidents ▪ 55 % decreased the number of incidents of sabotage by more than 20 % ▪ 53% decreased downtime resulting from security incidents by more than 20% ▪ 45% decreased the number of failed audits by more than 20% ▪ 42% decreased penalties from failure to comply with regulations by more than 20%

Definition of Maturity Class	Mean Class Performance
<p>Industry Average: Middle 50% of aggregate performance scorers</p>	<ul style="list-style-type: none"> ▪ 14% reduced the number of security incidents by more than 20% ▪ 4% decreased the cost of help desk support attributed to security incidents by more than 20% ▪ 86 % report 10 or fewer malware infections ▪ 67% report zero of data loss incidents ▪ 7% decreased the number of incidents of sabotage by more than 20% ▪ 15% decreased downtime resulting from security incidents by more than 20% ▪ 4% decreased the number of failed audits by more than 20% ▪ 4 % decreased penalties from failure to comply with regulations by more than 20%
<p>Laggard: Bottom 30% of aggregate performance scorers</p>	<ul style="list-style-type: none"> ▪ 0% reduced the number of security incidents by more than 20% ▪ 0% decreased the cost of help desk support attributed to security incidents by more than 20% ▪ 73 % report 10 or fewer malware infections ▪ 40% report zero data loss incidents ▪ 2% decreased the number of incidents of sabotage by more than 20% ▪ 0% decreased downtime resulting from security incidents by more than 20% ▪ 2% reduced the number of failed audits by more than 20% ▪ 0% decreased penalties from failure to comply with regulations by more than 20%

Source: Aberdeen Group, January 2008

The Best-in-Class PACE Model

Effectively protecting an organization requires a combination of strategic actions, organizational capabilities, and enabling technologies. Many organizations we interviewed indicated use of a strategy of "defense in depth," providing layers and redundancies that improve their security.

"We intentionally create a heterogeneous environment so that a would-be hacker doesn't have an easy time of it. We mix operating systems, servers, and firewall protections," says the CIO of bank that has been using managed security services for years.

The CIO of a Fortune 500 company applies a "defense in depth" strategy to their MSSPs as well, providing additional layers of protection or at least deterrence that bolsters the overall security.

Table 2: The Best-in-Class PACE Framework

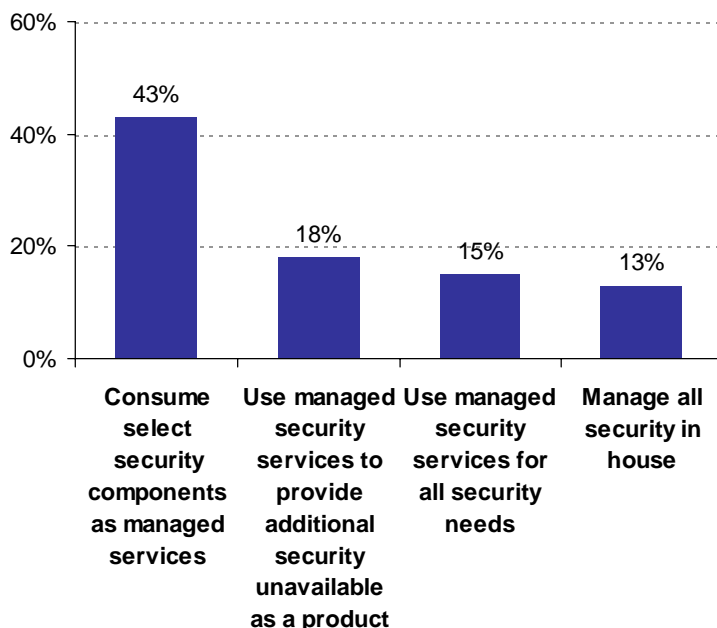
Pressures	Actions	Capabilities	Enablers
<ul style="list-style-type: none"> Need to improve security in the face of escalating threat 	<ul style="list-style-type: none"> Consume select security solutions as a managed service Use managed security services to provide solutions unavailable in-house 	<ul style="list-style-type: none"> Defined process for determining if a solution could or should be consumed as a managed service Regular, scheduled communications with MSSP Defined process for regularly re-evaluating technology purchase / subscription Key person or committee tasked with evaluating the suitability of managed services Portal or dashboard detailing status of managed security service Comprehensive audit trail 	<ul style="list-style-type: none"> Managed email security Anti-botnet services Authentication services Denial of service identification and remediation services Penetration testing services Managed security information and event management Vulnerability scanning services Intrusion detection and prevention services Unified threat management as a service

Source: Aberdeen Group, January 2008

Best-in-Class Strategies

Only 20 % of Best-in-Class organizations use managed security services for all their security needs. The others use a mix of managed security services and security solutions installed in-house. Sixty percent (60%) of Best-in-Class organizations have a key person or committee tasked with evaluating and choosing solutions and defined process for determining if a solution could or should be consumed as a service.

Figure 2: Best-in-Class Strategies for Consuming Managed Security Services



Source: Aberdeen Group, January 2008

Although 13% of Best-in-Class companies claim that their strategy is to keep all security in-house, none in fact do so. Each Best-in-Class organization consumed some managed security services as part of their overall defense.

Strategies For Determining Which Solutions to Consume as a Managed Service

Use managed security services for any kind of protection that is better done "in the cloud" - that is, anything that is better detected by aggregated events or traffic, and better detected from the provider's visibility across networks and accounts. Key examples include:

- **Email security.** The security service most widely deployed by the Best-in-Class. Forty-seven percent (47%) of the Best-in-Class use managed email security. Managed email security allows instantaneous upgrades to spam and virus identification and can prevent malicious email from ever reaching an organization. Because email is a universal need and because much of email security is better handled outside the organization, it's a good choice as a first security service to adopt.
- **Anti-botnet solutions.** Botnet activity is very difficult to detect from an individual machine. Anti-botnet services are the services highest on the list of managed services to acquire in the next 12 months, with a planned adoption of 12%.
- **Denial of service identification and remediation.** Denial of service attacks can and should be identified long before they reach their target, but it takes a service that can see and identify the activity on the network.

Use managed services for specialized services that you can consume as a service, perhaps on demand, more economically than you can deploy and manage in house. For example, with the demand for stronger authentication rising, using an authentication service that can handle various types of multi-factor authentication can greatly enhance your security without increasing the burden on your staff. Organizations that have foregone using PKI because of the significant investment required to deploy it can avail themselves of PKI on demand for a fraction of the cost.

Any solution that requires 24x7 attention for which you do not already have staff or expertise should be considered a target for outsourcing.

Also, consider outsourcing functionality that is new to the market. Products that provide new functionality that may ultimately be wrapped up into larger solution offers can be good candidates for outsourcing. Consuming these solutions as a service can prevent investment in assets that require training and may soon become obsolete. Switching from one service to another doesn't mean re-training. Solutions training is in the hands of the MSSP.

"We were looking for security, the ability to lock down the Internet and know where our employees have gone, but didn't want to pay a 100K/yr to get it. We chose this MSSP for these specific capabilities but we love it so much that it's now used by HR to create productivity reports and used by IT to identify heavy bandwidth usage. They are 'Johnny on the spot' with support – we've never had to wait more than half an hour for a response to our email or phone call. I compare that to another provider for which we had 'platinum service' – and it was horrible."

~ Director of IT,
Highly Federated Global
Business Organization

In the next chapter, we will see what the top performers are doing to get the best security.

Chapter Two: Benchmarking Requirements for Success

Each organization must determine its overall security strategy, weighing carefully its available resources and its actual risk.

Case Study — MNB Bank, Malvern, AR

We asked Kevin Hunt, Associate VP, Network Operations, for MNB Bank in Malvern, Arizona, about their experiences outsourcing security. For starters we asked how they determined what aspects of their security to outsource.

“We considered first the level of expertise of our current IT staff. Between us we have more than six decades of experience including a good understanding of security on our core systems, strong hardware skills, networking and hands-on network protection.” But that still left gaps in their knowledge base.

“Realizing we simply do not have the expertise on staff to properly protect ourselves, we did risk assessment studies. We realized training would be expensive, time consuming, take too long, and would never end.”

In addition Hunt tries to stay abreast of attack trends. “There really is no way to prepare for everything, but I do try to at least stay abreast of the ‘experts’ foreseeable trends. I want to be able to have somewhat intelligent conversations with my contacts at my MSSP, GFM, and especially the OCC. Of particular interest to me are the future possible attacks on VoIP systems, which we recently implemented. You can mark this down: VoIP is a messaging medium in which future spam attacks are certain. By knowing that, we included the means to switch from our phone system back to POTS lines in about one heartbeat.”

We asked how they determined what the cost should be. “We used our risk assessment to determine cost. What would it do to the reputation of the bank if private customer information were ever to be stolen? How would we ever win back our customer confidence? Asking questions like this, I got the green-light to find out what we needed.”

Their biggest obstacle? “Educating our board of directors and senior management without sounding like alarmists. Once we showed them in a calm and logical manner that there were better things to spend the bank’s money on than lawsuits, it was pretty simple, really.”

Their biggest surprise? “Finding out just how unprepared most of our financial institutions really are! Considering it would be hard to find a more regulated industry, I am amazed at the lack of a premium put on IT. The typical IT department for a bank of our size is responsible for everything from the phone system, core financial apps, system maintenance, software rollouts and updates, disaster / recovery planning and testing, laser printer maintenance, batch scheduling, employee security settings, and the list goes on forever. Doesn’t really leave much time for serious attention to be paid to attacks from oftentimes well-organized and coordinated cyber criminals... We rely heavily on our MSSP - our MSSP rocks!”

Fast Facts

- √ 65% of Best-in-Class organizations have SLAs in place with their MSSPs
- √ Best-in-Class organizations are 43% more likely than Industry Average and 57% more likely than Laggard organizations to measure the cost and efficiency of their MSSPs

Competitive Assessment

Aberdeen Group 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 performance levels, each class also shared characteristics in five key categories: (1) **process** (the approaches they take to execute their daily operations); (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 effective deployment of those tools); and (5) **performance management** (the ability of the organization to measure their results to improve their business). 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: The Competitive Framework

	Best-in-Class	Average	Laggards
Process	Defined process to determine whether a solution could or should be consumed as a managed security service		
	59%	50%	29%
Process	Defined process for regularly re-evaluating technology purchases and subscription choices		
	47%	42%	31%
Organization	Key person or committee tasked with evaluating the suitability of managed services		
	60%	56%	44%
Organization	Open and established communications with MSSPs		
	74%	64%	56%
Knowledge	Portal or dashboard detailing status of managed security services		
	50%	36%	16%
Knowledge	Comprehensive audit trail		
	56%	42%	31%
Technology	Integration between MSSP and other applications		
	45%	36%	11%
Technology	Managed email security		
	47%	35%	34%
Technology	Anti-botnet services		
	30%	16%	13%
Technology	Web filtering services		
	29%	27%	22%
Technology	Authentication services		
	25%	18%	12%
Technology	Security information and event management services		
	24%	18%	13%
Performance	Service Level Agreements (SLAs) with your MSSPs		
	64%	56%	44%

Source: Aberdeen Group, January 2008

Capabilities and Enablers

Based on the findings of the Competitive Framework and interviews with end users, Aberdeen's analysis of the Best-in-Class demonstrate their assessment of consuming security as a managed service is reflected across all aspects of our competitive framework

Process

Best-in-Class organizations have defined criteria for determining what kinds of security they need, what solutions are available, and what meets their needs. Requirements and resources vary widely from organization to organization, so there is no one methodology appropriate for all institutions. The important piece is to establish a process that's right for your organization and use it. Forty-seven percent (47%) of Best-in-Class organizations have a defined process in place to regularly re-evaluate their choices. As technologies mature, often functionality expands and prices drop. Organizations that do not continually re-evaluate are likely spending too much for too little.

Organization

Choosing managed security services and ensuring the success of your choice needs focused attention. Someone or a group of people need to take ownership for the choice and performance of the managed service providers you choose. Sixty percent (60%) of Best-in-Class organizations have a key person or committee tasked with evaluating the suitability of managed services.

MSSPs are not all alike, and price should not be your ultimate criterion. This person or group must be responsible for setting selection and performance criteria as well as enforcement and re-evaluation. The more successful organizations point to ongoing conversation, established rapport and ultimate trust in their MSSPs. Seventy-four percent (74%) of the Best-in-Class have regularly scheduled communication with their MSSPs.

Knowledge Management

Visibility into both the MSSP's performance and the security activity specific to your organization is critical to keeping your organization secure. Different providers provide different levels of visibility and interaction, some allowing great flexibility by offering different capabilities under one management framework. For example, you may want to monitor your redundant, back up systems but not put them under the same high-availability service level as your production environment.

Best-in-Class organizations out-perform all other respondents both in the fewest number of failed audits in absolute figures (86% of Best-in-Class companies report zero failed audits) and the greatest reduction of failed audits as a percentage decrease (45% of Best-in-Class companies reduced the number of failed audits by 20% or more). Clear, independent audit trails

"We really try to avoid MSSPs that intersect. If there are continuous processes, we'd opt for trying to get one MSSP - easier to manage. If there are multiple MSSPs doing different functions, generally my group manages them. But I don't own security operations. So if IT ops decided to outsource firewall management, I would be very interested, and I would have process ownership of FW rule changes, but IT OPS would probably manage that from a service delivery perspective."

~ Vice President
Multi-billion Dollar
Insurance Firm

help enormously in providing the documentation needed to pass audits. Additional reporting is helpful in identifying trends and forensic research.

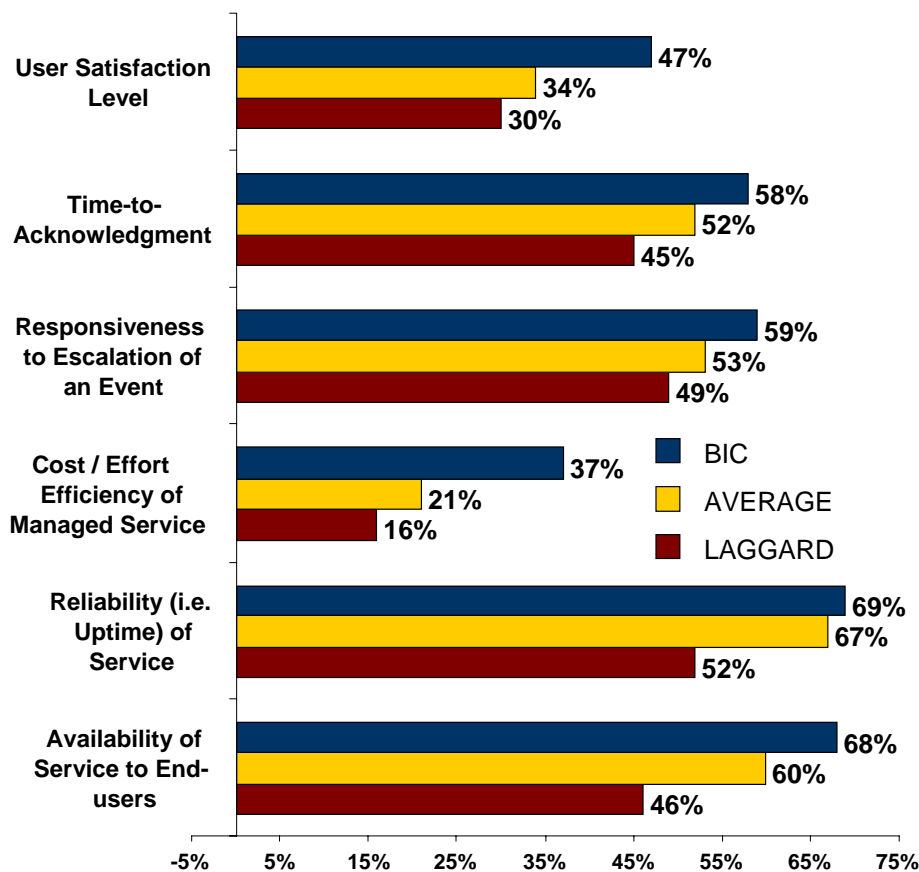
Technology

Forty-five percent (45%) of Best-in-Class companies have integrated their MSSPs with their other applications compared with 28% of all organizations. Some claim that this is no big deal. Others make a point of trying to avoid overlapping services - services that might be available from more than one provider whose services you consume - to avoid conflicts of jurisdiction and responsibility.

Performance Management

To ensure that MSSPs deliver on their promises, 64% of Best-in-Class organizations use SLAs. SLAs cover a lot of different aspects of service. Figure 3 illustrates some of the metrics that Best-in-Class organizations use to a greater extent than other organizations.

Figure 3: Types of Service Level Agreements



Source: Aberdeen Group, January 2008

Aberdeen Insights — Choosing (and Managing) your MSSPs

Regardless of the type of security services you choose to consume, use these guidelines in selecting MSSPs that will partner with you for your success:

1. Thoroughly vet your potential MSSPs. Critical to your success is your MSSP's responsiveness to your problems. In every interview with survey respondents, Aberdeen found that the MSSP's responsiveness was cited as the most important factor. Great responsiveness was reflected in highly satisfied, loyal customers - some who have used the same MSSP for 10 years now. Positive experience consuming one kind of security service from an MSSP over time can make an organization open to exploring more services from the same MSSP. Lack or responsiveness made angry, frustrated customers look for new providers.

Due diligence is worthwhile for each prospective MSSP, including speaking to their customers that are most like your organization. Think about the size of your organization and the kind of MSSP that's going to give your organization the best service. Consider local and regional providers as well as the big guys - be sure your provider is going to service your organization.

2. Don't make cost your ultimate consideration. A long-time veteran of using MSSPs says that sometimes what looks like a good deal isn't. "That 10% we thought we were saving ended up costing us 50% to 100% more in time and frustration. Ultimately we lost millions and we had to intervene and take it back into our own hands. I always consider outsourcing - I just won't consider those MSSPs that can't provide adequate support."
3. Establish well-understood SLAs with your providers. For example, one bank Aberdeen interviewed thought that their guaranteed response time was four hours only to learn in the hour of need that the MSSP would "try" to respond within four hours but guaranteed 24. Losing a million dollars a day became a costly lesson in reading the fine print.

Other guidelines include:

- Establish a process to measure compliance with your SLAs
- Do pre-emptive planning to deal with the most likely risks
- Schedule regular communications with your managed security services providers
- Establish an escalation plan and known course of action to enforce SLA compliance
- Establish redundant communications with your MSSP

"At some point you have to manage some point of your security, unless you're so small you can't afford to. You may not have the skills in-house to even know the risk let alone manage the risk - you may need to actually outsource the assessment."

~ Mark Cummuta CIO,
Midwestern Community Bank

Chapter Three: Required Actions

Whether a company is trying to move its performance in managed security services from Laggard to Industry Average, or Industry Average to Best-in-Class, the following actions will help spur the necessary performance improvements:

Laggard Steps to Success

Although Laggard organizations widely deploy managed security services, they are getting inferior results. The following recommendations can help them improve their security:

- Use a portal or dashboard to gain visibility into security services. Only 16% of Laggard organizations currently use this capability.
- Proactively manage your MSSP. Only 44% of Laggard organizations have SLAs with their MSSPs (compared with Best-in-Class at 64% and Industry Average at 56%). Only 33% of Laggard organizations have a process in place to measure compliance with their SLAs and only 25% attempt to enforce them. Make sure you have SLAs that meet your needs and that your MSSP meets the SLA.
- Establish and enforce a defined process for regularly re-evaluating your technology purchase and subscription choices. Only 31% of Laggard organizations have such a process in place. Many now well-performing organizations that are content with their MSSPs had previously experienced less than satisfactory results before switching providers.

Industry Average Steps to Success

- Only 26% of Industry Average organizations consume any security solutions as a managed service, versus 100% of the Best-in-Class. An obvious first step is to identify those solutions that typically yield better results when delivered as a service because the threat is best identified with visibility across networks or across accounts. See Chapter One for where to begin.
- Only 7% of Industry Average organizations were able to reduce fraud by more than 20%, compared with 42% of Best-in-Class organizations. Bolster security by strengthening authentication. Experiment with various forms of authentication services to determine which are most effective for your organization without committing internal resources or locking yourself into one solution.
- Use a portal or dashboard to gain visibility into security services. Only 36% of Industry Average organizations currently use this capability.

Fast Facts

- √ 74% of Best-in-Class companies have regularly scheduled communications with their MSSPs
- √ Best-in-Class organizations are 43% more likely than Industry average and 57% more likely than Laggard organizations to measure the cost and efficiency of their MSSPs

Best-in-Class Steps to Success

- Measure your MSSPs against your performance expectations as outlined in your SLAs. Although the Best-in-Class are better informed than other organizations, 36% of the Best-in-Class either don't know or don't measure their MSSPs performance.
- Enforce your SLAs. Only 35% of the Best-in-Class currently enforce the SLAs that have with their MSSPs. Holding your MSSP accountable could improve your performance significantly.
- Explicitly measure the cost and efficiency of your MSSP. Only 41% currently use these criteria in evaluating their MSSP's performance. This data is integral to the ongoing re-evaluation needed to keep security up to date and costs in line.

"We started out with our MSSP in '98. We realized we needed a full service center because as a small company you can't do it all yourself. We've been a profitable ASP since day one because we are able spread our costs over all customers. We could never have done that (be 85% profitable) if we had to run all that ourselves."

~ CFO, ASP serving
Fortune 500 Energy,
Healthcare,
and Chemical Companies

Aberdeen Insights — Summary

The results of the current research into consuming managed security services are ground breaking. It's evident that Best-in-Class organizations recognize that they actually need managed security services as part of their portfolio of defense solutions. Using managed security services, Best-in-Class organizations demonstrated significantly better security performance across a spectrum of criteria - less data loss, fewer failed audits, less fraud, fewer security incidents in general, fewer incidents of sabotage, fewer malware infections, reduced help desk costs, and less downtime as a result of a security incident.

As the threat landscape continues to evolve, new solutions will continue to emerge to address them. It's likely that consuming new functionality as a service will become increasingly attractive - fewer pieces to manage in-house, less training, more flexibility around choice, greater protection from certain kinds of attacks, and access to services on-demand that are otherwise out of reach.

Organizations need to determine their greatest areas of risk and consider the possibility of addressing these risks with managed services. However, all organizations need to establish criteria and process for choosing these services and ensuring the ongoing success of using them. Managed security services are not of themselves a panacea, but care, planning, and choice can make the seeming impossible and unaffordable task of contemporary IT security possible, affordable, and ultimately less worrisome than what most organizations experience today.

Send to a Friend 

Appendix A: Research Methodology

Between December 2007 and January 2008, Aberdeen examined the use, the experiences, and the intentions of more than 180 organizations deploying a diverse set of security solutions both as installed software and as managed security services.

Aberdeen supplemented this online survey effort with interviews with select survey respondents, gathering additional information on managed security services strategies, experiences, and results.

Responding enterprises included the following:

- *Job title / function:* The research sample included respondents with the following job titles: C-level executives, CEO, CIO, CFO, etc. (32%); Vice President (8%); Director or Manager (43%) staff, consultants, and other (17%).
- *Industry:* The research sample included respondents from High Technology/Software (27%); Telecommunications Services (12%) Finance Banking and Accounting (9%); Computer Equipment and Peripherals (8%); Education (7%) and all others (37%).
- *Geography:* The majority of respondents (58%) were from North America. Remaining respondents were from the Asia-Pacific region (19%), EMEA (17%), Central/South America and Caribbean (6%).
- *Company size:* Sixteen percent (16%) of respondents were from large enterprises (annual revenues above US \$1 billion); 34% were from midsize enterprises (annual revenues between \$50 million and \$1 billion); and 50% of respondents were from small businesses (annual revenues of \$50 million or less).
- *Headcount:* Thirty-four percent (34%) of respondents were from large enterprises (headcount greater than 1,000 employees); 24% were from midsize enterprises (headcount between 100 and 999 employees); and 42% of respondents were from small businesses (headcount greater than 1,000 employees).

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.

Study Focus

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

- √ The extent to which managed security services are being consumed
- √ The effectiveness of managed security services versus security maintained strictly in-house
- √ Best practices in choosing and managing MSSPs
- √ Their plans for future investment in particular security solutions as well as their preference for how this solutions will be delivered

The study aimed to identify emerging best practices for consuming managed security services and to provide a framework by which readers could assess their own strategies around consuming managed security services.

Table 4: The PACE Framework Key

Overview
<p>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:</p> <p>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)</p> <p>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)</p> <p>Capabilities — the business process competencies required to execute corporate strategy (e.g., skilled people, brand, market positioning, viable products / services, ecosystem partners, financing)</p> <p>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)</p>

Source: Aberdeen Group, January 2008

Table 5: The Competitive Framework Key

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

Source: Aberdeen Group, January 2008

Table 6: The Relationship Between PACE and the Competitive Framework

PACE and the Competitive Framework – How They Interact
<p>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.</p>

Source: Aberdeen Group, January 2008

Appendix B: Related Aberdeen Research

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

- [Securing the Online User Experience - Building Customer Confidence and Stopping Fraud](#); December 2007
- [The Ins and Outs of Email Vulnerability](#); July 2007
- [Thwarting Data Loss](#); May 2007

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

Author: Carol Baroudi, Research Director, IT Security,
carol.baroudi@aberdeen.com

Founded in 1988, Aberdeen Group is the technology- driven research destination of choice for the global business executive. Aberdeen Group has 400,000 research members in over 36 countries around the world that both participate in and direct the most comprehensive technology-driven value chain research in the market. Through its continued fact-based research, benchmarking, and actionable analysis, Aberdeen Group offers global business and technology executives a unique mix of actionable research, KPIs, tools, and services. This document is the result of primary research performed by Aberdeen Group. Aberdeen Group's methodologies provides 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.

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>

010108a