MANAGED SECURITY SERVICES: WHEN IT'S TIME TO STOP GOING "IT" ALONE

August 2014

→ **Derek E. Brink,** CISSP, Vice President and Research Fellow, IT Security and IT GRC

Report Highlights

p2

Security is important, but is it strategic? Ask if management of security activities is the best use of your staff's time and expertise.

p3

Addressing important aspects of IT Security requires leveraging the overwhelming volume of data and data sources that already surrounds us.

p6

Aberdeen's research indicates high growth for managed security services, as more companies realize they're better off not "going IT alone."

p7

Aberdeen's analysis shows that the annual cost advantage for managed security services over that of in-house is as high as 50%.

Even if a given organization is capable of the traditional, do-it-yourself integration of on-premise security solutions using in-house resources, is it really better off doing IT on its own – or would it be better off leveraging the expertise, scale and scope of a third-party service provider? In a comparison of the annual cost of traditional security implementations with that of managed security service providers, Aberdeen's research showed the annual cost advantage for managed security services to be as high as 50% per year.

ABERDEEN GROUP
A Harte Hanks Company

Security-related activities are clearly important, but are they strategic? Asked another way, is management of certain security activities the best use of your staff’s time and expertise?

Business Context: Security is Important, But is it Strategic?

It’s not hard for any given organization to acknowledge that the following security-related activities are *important*:

- ➔ Ensuring that IT infrastructure, intellectual property and sensitive data are well-protected
- ➔ Keeping up with the latest security threats and vulnerabilities
- ➔ Monitoring, detecting, investigating and responding to security incidents and events in a timely manner
- ➔ Keeping installed security solutions up-to-date
- ➔ Satisfying compliance requirements – and auditors –in a cost-effective manner

The more difficult question is this: are these activities *strategic*?

This is not just some kind of frivolous wordplay. By *important*, we mean that it has serious value; it requires and deserves serious attention. By *strategic*, we mean that it relates to the achievement of long-term interests, advantages and objectives. Many things can be important, but not strategic – for example, a company may decide that it’s important to provide their direct sales force with company cars, but that the provisioning and regular maintenance of company cars is not so strategic to their mission that they should perform these functions in-house, by vertically integrating a fleet services function. Aberdeen has written about this concept many times in the context of IT Security, in discussions of the *unrewarded* risks of security and compliance versus the *rewarded* risks of innovation and growth.

The question can be asked another way: is management of these security activities the best use of your staff’s time and expertise?

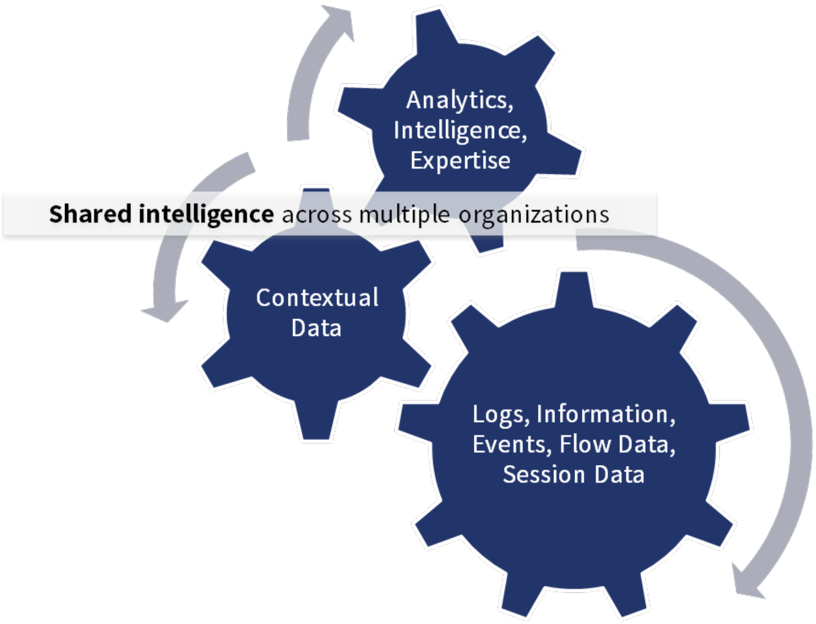
A Classic Build vs. Buy Decision

Frame the question however you like, what we're talking about here is fundamentally a "build versus buy" decision, that is:

- The traditional, do-it-yourself integration of on-premise security solutions by the organization's in-house resources, versus
- Leveraging the scale and expertise of a managed security service provider (MSSP).

To illustrate the point, consider the overwhelming volume of data and data sources that organizations can and should be leveraging to carry out the important activities enumerated on the previous page (Figure 1).

Figure 1: Addressing Important Aspects of IT Security Requires Leveraging the Overwhelming Volume of Data and Data Sources That Already Surrounds Us


Analytics, Intelligence, Expertise
Shared intelligence across multiple organizations
Contextual Data
Logs, Information, Events, Flow Data, Session Data

Source: Aberdeen Group, August 2014

Definitions

Managed Security Service Providers (MSSPs) offer services such as management, monitoring, testing and incident response for one or more specific IT Security solution categories (e.g., intrusion detection / prevention, log management, incident and event management, network monitoring).

MSSP functionality may be delivered by on-premise systems (e.g., appliances which are remotely managed), over the Internet, or a hybrid.

➔ *Logs* record information about the events that take place throughout the organization's **IT infrastructure**:

- Network devices
- Servers (physical, virtualized and cloud)
- Endpoints
- Operating systems
- Applications
- Databases

➔ *Logs*, *information*, *events*, *flow data* and *session data* are also generated by the organization's existing **security solutions**:

- Network firewalls
- Intrusion detection / prevention systems
- Unified threat management systems
- Web application firewalls
- Anti-virus software
- File integrity managers
- Identity and access management

➔ Gathered data can be enriched with **contextual information**:

- Assets
- Vulnerabilities
- GeoIP

  - Third-party blacklists
  - Users (e.g., privileged, non-privileged)

- ➔ **Advanced analytics** can be used to generate *insight*:
  - Anomaly detection
  - Statistical analysis
  - Heuristic analysis
  - Threat intelligence
  - Security experts
- ➔ The most mature organizations also use **shared intelligence**, which is integrated across multiple organizations

All of the above ties back to our same questions: yes, these activities are important – but is it really strategic for my organization to perform all of these functions itself? Even if my organization is capable of managing all of this complexity, would it really be better off doing it on its own – or would it be better off leveraging the expertise, scale and scope of a third-party service provider?

Aberdeen's Research Findings: Market Trends Show High Growth in Managed Security Services

Aberdeen's benchmark research helps to show how the market has been answering these questions thus far, and how organizations intend to answer them going forward. Respondents to Aberdeen's surveys indicate very strong growth in managed security services – in fact, the majority of new deployments are choosing managed security services over in-house implementations, as summarized in Table 1.

Table I: Aberdeen's Research Indicates High Growth for Managed Security Services, as More Companies Realize They're Better Off Not "Going IT Alone"

	Overall		In-House		Managed Services	
Security Solution Category	**Current Adoption**	**Planned Growth**	**Current Adoption**	**Planned Growth**	**Current Adoption**	**Planned Growth**
Log Management	**78%**	13%	68%	*2%*	9%	**88%**
Security Information and Event Management	**74%**	16%	65%	*3%*	9%	**112%**
Security Monitoring	**72%**	18%	54%	*3%*	18%	**63%**
Security Analytics	**56%**	30%	48%	*15%*	8%	**121%**

Percentage of Respondents (N=180)
Source: Aberdeen Group, August 2014

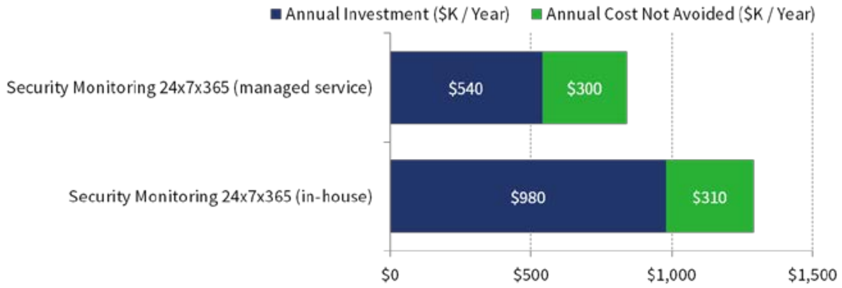
Using the security solution categories of log management, security information and event management (SIEM), security monitoring and security analytics as examples, Aberdeen's research findings show how the market is answering these questions. Yes, these activities are important – a majority of respondents have implemented solutions in these areas. No, these activities are no longer being viewed as strategic – the vast majority of new implementations are opting for managed security services.

Why the Growth is in Managed Security Services

Aberdeen's research not only reflects the market's movement towards managed security services from a strategic perspective, but also provides some insight into the financial motivations behind this momentum. By comparing the annual cost of traditional, on-premise implementations with that of managed security services implementations, the annual advantage for managed security services is found to be as high as 50%.

In the specific case of **24x7x365 security monitoring**, Aberdeen's analysis shows that the annual total cost advantage for managed security services over in-house implementations is about 35% per year (Figure 2).

Figure 2: For the Specific Case of 24x7x365 Security Monitoring, the Annual Cost Advantage for Managed Security Services over In-House Implementations is About 35% / Year



(total annual cost not avoided) = (average number of security-related incidents experienced in the last 12 months) x (average total cost per incident); (total annual cost) = (annual investment) + (annual cost not avoided)
Source: Aberdeen Group, August 2014

In security monitoring – and in several other solution categories for which sufficient responses were available for a meaningful comparison – MSSP was the clear winner over in-house deployments. In addition, the organization's own in-house resources are freed up to pursue other, more strategic tasks.

Solutions Landscape (illustrative)

Managed security service providers for the solution categories referenced in this report can range from smaller specialists to multi-billion dollar global firms; following is an illustrative list:

NEC Managed Services
Solutionary
Dell SecureWorks
Alert Logic
Symantec Managed Security Services

IBM Managed Security Services
Verizon Managed Security Services
HP Managed Security Services
BT Assure Managed Security Services
AT&T

Definitions

Annual Investment ($K / year) is what the organization spends to perform these security activities. For the respondents in Aberdeen's study, the MSSP deployments were significantly less expensive.

Annual Cost Not Avoided ($K / year) is security-related costs that the organization incurs, in spite of its investments (e.g., to respond to and recover from security-related incidents and disruptions). For respondents in Aberdeen's study, the MSSP deployments were slightly less expensive.

Total Annual Cost ($K / year) is the sum of Annual Investment and Annual Cost Not Avoided.

Summary and Key Takeaways

Security-related activities such as the following are *important* for your organization, but are they also *strategic*?

- ➔ Ensuring that IT infrastructure, intellectual property and sensitive data are well-protected
- ➔ Keeping up with the latest security threats and vulnerabilities
- ➔ Monitoring, detecting, investigating and responding to security incidents and events in a timely manner
- ➔ Keeping installed security solutions up-to-date
- ➔ Satisfying compliance requirements – and auditors –in a cost-effective manner

This question frames a fundamental "build versus buy" decision for the deployment of corresponding security solutions:

- ➔ The traditional, do-it-yourself integration of on-premise security solutions by the organization's in-house resources, versus
- ➔ Leveraging the scale and expertise of a managed security service provider (MSSP)

To illustrate the point, consider the overwhelming volume of data and data sources that organizations can and should be leveraging to carry out these important activities:

- ➔ *Logs* that record information about the events that take place throughout the organization's **IT infrastructure**
- ➔ *Logs*, *information*, *events*, *flow data* and *session data* that are generated by the organization's existing **security solutions**

- **Contextual information** that enriches gathered data
- **Advanced analytics** that generates *visibility* and *insight*
- **Shared intelligence** that is sourced across multiple organizations

Even if a given organization is capable of managing all of this complexity, would it really be better off doing it on its own – or would it be better off leveraging the expertise, scale and scope of a third-party service provider?

Using the security solution categories of *log management*, *security information and event management (SIEM)*, *security monitoring* and *security analytics* as examples, Aberdeen's research findings show how the market is answering these questions:

- Yes, these activities are important – a majority of respondents have implemented solutions in these areas
- No, these activities are no longer being viewed as strategic – the vast majority of new implementations are opting for managed security services

Aberdeen's research not only reflects the market's movement towards managed security services from a strategic perspective, but also provides some insight into the financial motivations behind this momentum:

- By comparing the annual cost of traditional, on-premise implementations with that of managed security services implementations, the annual advantage for managed security services is found to be as high as 50%
- In the specific case of **24x7x365 security monitoring**, Aberdeen's analysis shows that the total annual cost

advantage for managed security services over in-house implementations is about 35% per year

- In addition, the organization's own in-house resources are freed up to pursue other, more strategic tasks

For more information on this or other research topics, please visit www.aberdeen.com.

Related Research

Why are Small Businesses Moving to Cloud Backup and Recovery?; May 2014

Network Security: Why the Growth is Moving from In-House to Managed Services; May 2013

Incident Response: Detecting and Containing Earlier in the Attack Lifecycle; March 2013

Network Security: Firewalls Alone are Not Enough; April 2012

Security and Cloud: Adoption of Security Software-as-a-Service; August 2011

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

About Aberdeen Group

For 26 years, Aberdeen Group has published research that helps businesses worldwide improve performance. We identify Best-in-Class organizations by conducting primary research with industry practitioners. Our team of analysts derives fact-based, vendor-neutral insights from a proprietary analytical framework independent of outside influence. The resulting research content is used by hundreds of thousands of business professionals to drive smarter decision-making and improve business strategy.

Aberdeen's content marketing solutions help B2B organizations take control of the Hidden Sales Cycle through content licensing, speaking engagements, custom research and content creation services. Located in Boston, Massachusetts, Aberdeen Group is a Harte Hanks Company.