Managed Security Services: A Primer

Summary

Managed Security Services are defined as those offerings a Managed Security Service Provider proposes as part of a comprehensive suite of outsourced security services. These services include: Firewall configuration and monitoring; IDS/IPS configuration and monitoring; Log analyses and reporting; Antivirus management; Web content controls; Virtual Private Network (VPN) management; Anti-spam protection; Data Loss Prevention (DLP); Application controls; and Professional Security Services (Figure 1). MSSPs can be differentiated by the scope of their service portfolios, the quality of the tools they deploy to support those services, their capability to deliver the appropriate customized security solutions, the velocity of their threat response, and the quality of the professional service experts they employ to manage these solutions.

In this document, we present a definition of Managed Security Services (MSS) and MSS Providers (MSSPs). We will discuss the motivations that underlie the choice to outsource, the evolution of Managed Services (MS), and the trend in IT towards Utility Computing and Cloud-based services. We will conclude by showing that information is most effectively secured when expert security professionals are able to analyse data generated by an appropriate combination of world-class hardware and software. In doing so, we hope to provide you with the information and understanding that you will need when choosing a MSSP that best satisfies your organization’s security requirements.
Introduction

Most definitions of Managed Security Services (MSS) begin by citing case after case of terrifying security incidents, backed by a laundry list of guess-timated loss statistics usually provided by one vendor or another. The goal, in these cases, is to scare the reader – to create fear, uncertainty and doubt (FUD), which is hoped to motivate the purchasing centers in the reader’s mind. There normally follows a bullet list of security point solutions such as firewall management or antivirus deployment that claim to protect the reader’s organization from ending up on the case list mentioned above. There is seldom a discussion concerning the means by which these point solutions are interrelated and managed; financials are vaguely mentioned other than that MSS will save the reader money; metrics are ignored for the most part; and an overall definition of MSS is generally left to the reader’s imagination.

There is no question that in this contemporary networked world, security is hard, and its practitioners often fail or are thwarted by undereducated (in the sense of security) users, perennially inadequate resources, and myopic management. In the very near future (the next 1-3 years), as network boundaries continue to dissolve under the stampede to Cloud, mobile, and virtualized infrastructure, and as applications and their cognate databases pop up on everything from phones to tablets to toasters, it is difficult to imagine a scenario in which rationally and economically securing all of these data becomes any easier. In fact, it is a straightforward matter to argue that most of the security tools and processes that we have relied upon are simply not up to the task of protecting critical data on Internet 2.0.

In order to endure and compete, organizations are going to require resources, expertise, tools, policies, processes, and procedures that, frankly, most will not be able to afford. In addition, many of these organizations exist within verticals that are subject to an increasingly complex and changing regulatory environment – the key drivers here being, FISMA, SOX, HIPAA/HITECH, Basel II, and PCI compliance.
Organizations will need help – and that help will be in the form of the Managed Security Service Provider (MSSP).

What elements are included under the umbrella term, Managed Security Services? What defines an effective Managed Security Service Provider? Why would an organization utilize these services? In this document, our goal is to provide you with the answers to these three questions. In addition, our intention is to provide you with the fundamental knowledge surrounding these terms in order to enable you to rationally determine if you require these services, which subset of these services will satisfy your requirements, when you need them, and, finally, how to optimally acquire MSS.

The Evolution of Managed Security Services

Managed Services
Before exploring the evolution of MSS, it is instructive to review the history and development of Managed Services. Managed Services (MS) are those services that an organization chooses to outsource. Why outsource anything?

A simple example: John and Jill Smith are co-workers in IT at General Products Corp. Their core competence is working hard in order to support, grow, and secure their family. Because they are both resource and time constrained, they are obligated to outsource, relatively low priority, periodic, tasks such as house cleaning, automobile maintenance, and lawn care; as well as the critical task of childcare for their two children. These are variable costs in that these costs grow proportionally to the activity. In addition, the Smiths assume a proportion of fixed costs – in that they outsource, at times, the services of the police, fire fighters, doctors, dentists, etc. The costs of these services are shared among the population since these services are used only occasionally – when they are needed - and it is silly (not cost effective) to imagine them hiring a doctor full-time, or a police officer to watch their home 24x7 in case they might be burgled.

In terms of the enterprise - according to this approach - if a company can concentrate all of its investment and energy on the one thing it does best and hand off everything else to partners; it can achieve unprecedented levels of efficiency, speed, and quality. The core competence can be almost anything - from brand management to widget production to flipping burgers.

The MS industry grew to fill this role. Initially, managed services contracts mimicked classic utility contracts, and centered on fairly complex and personalized arrangements between Telco’s and large enterprise clients as these clients sought to offload their telecommunications infrastructures (costs). The next step in the evolution of MS saw a large number of small – now, mostly vanished - companies who focused on providing services for outsourcing various components of IT. These managed services included: backup and storage, firewall administration and monitoring, network management, user management, desktop support, and help desk, and were characterized by the emergence of SLA’s, remote monitoring, dedicated MSP NOC’s, and the centralization of professional services in these NOC’s. The winners in this field were those MSPs who were able to best consolidate their strategies so as to provide their internal service groups with processes and tools whose actionable consequences provided the best customer experience.
The Cloud

As bandwidth increased, as servers and operating systems became commoditized, and pressure increased on IT groups to do more with less, these managed services were rebranded, and became the foundation of the shift to “On Demand” or “Utility” computing. Utility computing is the wrapping of computing resources, such as processor cycles, storage, I/O, or bandwidth, as a metered service similar to a traditional public utility (such as electricity, water, natural gas, or telephone network). This model has the advantage of zero or low initial investment in IT resources; instead, computational resources are essentially leased - turning what was previously a requirement to purchase, provision, and manage products (hardware, software and network bandwidth) into an on-demand service.

Utility computing is not a new concept, but rather has quite a long history. Fifty years ago – speaking at the MIT Centennial in 1961 – John McCarthy noted that:

“If computers of the kind I have advocated become the computers of the future, then computing may someday be organized as a public utility just as the telephone system is a public utility... The computer utility could become the basis of a new and important industry.”

Virtualization and a number of cloud computing models are further propagating the model of information usage, storage and transmission as a service or a group of interrelated services. Cloud computing is poised to change the economics of computing by replacing up-front CAPEX with a more scalable and variable cost structure based on an on-demand, elastic, pay-as-you-go model, in which traditional IT services – once regarded almost as the arcane practices of a technical voodoo cult – are transforming into commodity services.

Gartner predicts that by 2012, a fifth of all businesses will not own any IT assets. While this may be overstated, there is a clear trend toward moving to a hosted services model. Organizations who make this move are seeing immediate benefits in that they are able to economically tap into additional external expert resources to complement or supplement existing skill sets, especially for more complex IT implementations such as security. This is particularly true in the SMB space because although SMB’s are as likely as LE organizations to be victims of a cybercrime event, and although they do business within the same regulatory environment as LE’s, most SMB’s do not have the resources to implement the blend of security controls required in the contemporary networked world.

Managed Service Providers who will define, “Best-in-Class” in this arena are those who will be able to distinguish their offerings by linking their value propositions to a real difference in how they align their internal people, processes, and tools with the requirements of their customers. After all, managed service providers have been providing cloud-like services for years - well before it became fashionable to prepend the term, “Cloud” to all things Internet that are not CPE.
The Challenge of Security Services

As we have said earlier, IT security is hard. True professionals in information security must be expert in a number of fields including: networking, programming, and operating systems. These individuals do not grow on trees, nor do they come cheaply.

Information security is business-critical – a single error can lead to catastrophic consequences. Threats, risks, and regulations evolve - becoming more complex with every iteration. With the exception of some botnet malware such as Zeus and its sibs, threats are diverse; and, in fact, are often targeted at a small subpopulation of victims. No one is immune, and SMBs are equally as vulnerable as large enterprise organizations. No particular static countermeasure or suite of countermeasures will secure an organization. Security is a war, and like any other war, is characterized by a spiral of innovation and counter-innovation. It is trite to define security as an on-going process, but in this case, trite is true. The practice of protecting information is, simply, not automatable. Ultimately, humans are the attackers, and human experts must - with the assistance of best-in-class, expert tools - relentlessly commit to its protection.

The sensible application of information security controls defines critical corporate assets and protects their integrity, ensures compliance with industry and government regulations, maintains the legitimacy of a trusted brand image and sustains business continuity. However, providing an appropriate level of security (deciding how much to invest and more importantly, where to place those investments) requires a combination of state-of-the-art technology, experienced personnel, proven processes, and continuous threat intelligence that few organizations can afford (See Table 1).

Management is faced with the realization that although reliably securing information assets is a core requirement, it is not a core competency. Thus, organizations begin to investigate MSS & MSSP’s, and if they are new to this, they may be overwhelmed at first.

Table 1. Difficulties associated with building reliable in-house security solution

<table>
<thead>
<tr>
<th>Costs</th>
<th>The barriers to entry in this field are high, regardless of the proposed architecture. The initial costs to acquire appropriate hardware and software tools, combined with building out the physical infrastructure to house a Security Operations Center (SOC) are significant. In addition, hardware must be upgraded, maintained, and powered; software licenses are normally renewed annually; and salaries for expert support often exceed normal technical ranges.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Staffing</td>
<td>Security professionals must aggregate, monitor, and react to the data generated by the security tools on a 24x7x365 schedule. Finding, recruiting, training, and managing these individuals is difficult and expensive. Creating the business processes that these individuals must follow and monitoring compliance is time consuming and expensive as well.</td>
</tr>
<tr>
<td>Scaling</td>
<td>Considering the sheer volume of data produced by security devices and the potentially catastrophic consequences of a single mistake – many individuals are often required for appropriate analyses. Since threats and their vectors continue to proliferate, scaling hardware, software, processes, and human resources becomes inefficient for a single organization.</td>
</tr>
<tr>
<td>Experience</td>
<td>Within a single organization, a determined attack is often regarded as a sensational event, and until cooler heads prevail, protective and reactive processes</td>
</tr>
</tbody>
</table>
are thrown out the window. A chaotic response (from both a technical and business perspective) often causes more damage to the organization than the attack itself. Also, an organization has a narrow view into the current Internet environment; thus, its awareness of evolving threats is limited.

IT security outsourcing services (and products) can take many forms. Currently, numerous companies offer a smorgasbord of capabilities and products that they define as, “Managed Security Services.” Semantics in this field can be so confusing that industry analysts cannot agree on how to categorize the services offered - even the VP of a major MSSP has been quoted as saying, “the wide range of MSSPs and their offerings can prove daunting to compare and understand”. Company A manages firewalls. Company B offers ISO 27001 security policy development and training. Another recommends a CMS platform where security events can be aggregated. How does one make a rational decision in the current environment?

Choosing an MSSP

In order to simplify this process, we proposed a simple high-level definition of Managed Security Services above (Figure 1). These security services are the functional constituents of a suite of security services offered by world-class MSSP’s – within a framework defined by the following obligatory characteristics:

1. Comprehensive Portfolio
2. Supported by Best-in-Class Expert Tools
3. Monitored 7x24x365 by Expert (Certified) Security Professionals

MSS provide a unified solution for protecting data, for allowing secure communication across the Internet, for secure linkage with business partners, and for compliance with relevant regulatory statutes (Figure 2). From the point-of-view of the CIO, one of the most obvious business benefits of MSS is the ability to shift costs from CAPEX to more predictable OPEX. Business outcomes include: improved cost management, operational efficiencies related to scaling, mitigation of staffing risks, and business process improvements - while retaining enough management oversight and flexibility to respond to additional threats. In a nutshell, the tactical agility offered by MSS allows management to focus on strategic objectives.

Thus, not only do the security services delivered by the MSSP provide an organization with a greatly reduced threat surface, they also confer “future-proofing”; that is, a buffer from fundamental changes to the Internet - IPv6 migration, cloud technologies, mobility of data assets, virtualization, and botnets, for example – that are occurring or are certain to occur in the near future.

To mitigate your risk when choosing a MSSP, you should first evaluate your existing security infrastructure so that you begin discussions with a plan, to outsource where you have weaknesses or where your existing systems’ cost/benefit ratio is low, and to reinforce those areas where you have core strengths. If you have invested in a security hardware/software product, and can economically manage it, then continue to do so. “If it ain’t broke, don’t fix it”. One of the advantages to working with a world-class MSSP is that you should be able to pick and choose services from their portfolio.

When evaluating a MSSP, examine the market to identify a list of providers that have the capability to deliver the services you require. Assess how well each provider’s offering matches your requirements. Check that their
A hardware/software toolset is best-in-class – typically a unified platform rather than a proliferation of disparate small applications and appliances. Choose a MSSP that has a verifiable history within this market – a MSSP that has established a positive reputation with a well-defined set of professionals, tools and processes. Ask your potential MSSP vendor these five questions:

- Can you provide me with a copy of your SLAs?
- What are my requirements as a client?
- What percentage of my compliance requirements will these services provide?
- Can I retain the ability to manage this environment?
- Can you provide me with a list of organizations similar to mine (Case Studies, Press Releases, etc.)?

Then manage the deal according to the impact it will have on your business.

For additional information regarding recommended Managed Security Service Providers, please email us at: managedservices@i5sci.com.

---

**About i5 Scientific**

i5 Scientific is an IT development firm specializing in the architecture and security of both static and virtualized networks and applications.

We have seen that in today's IT environment, networking and security architecture is often a hodgepodge of hardware, software, processes and procedures that have evolved to mediate specific problems; and which, as a by-product of the process, have discounted both business value and coordinated, central management. Security assessments of these complex architectures are often performed by well-intentioned, but inexperienced individuals who use a single toolset to complete an essentially “commodity” audit. While this approach may suffice at a base level, it neglects the simple fact that all networks are unique, and that even the same physical network will differ with respect to connectivity and security characteristics over time.

At i5, we believe that the better approach is to focus on only a few organizations. Our approach is to utilize the appropriate tools to work with individuals within an organization from both a top-down (architectural) standpoint, and a bottom-up (assessment) standpoint.

To that end, we offer a growing menu of Security Consulting and Reseller offers. For additional information, please visit us at: [http://www.i5sci.com](http://www.i5sci.com).